IoMT Security: A Semantic Framework for Vulnerability Detection in Remote Patient Monitoring

Kulsoom Saima Bughio

This thesis is presented for the degree of
Doctor of Philosophy
School of Science
Edith Cowan University, Australia
June 2024

IoMT Security: A Semantic Framework for Vulnerability Detection in Remote Patient Monitoring

Submitted in total fulfilment of the requirements for the
degree of Doctor of Philosophy (Information Technology)

Kulsoom Saima Bughio

Supervisors

Principal Supervisor: Dr. David Michael Cook, School of Science ECU, Australia
Associate Supervisor: Dr Syed Afaq Ali Shah, School of Science ECU, Australia

School of Science,
Edith Cowan University, Australia

”Dedicate to my family, especially my beloved parents, Abdul Karim Unar and Fatima Unar, and my beautiful children, Sindhyar and Aizel.”

Abstract

The increasing need to safeguard patient data in Internet of Medical Things (IoMT) devices highlights the critical importance of reducing vulnerabilities within these systems. The widespread adoption of IoMT has transformed healthcare by enabling continuous remote patient monitoring (RPM), which enhances patient outcomes and optimizes healthcare delivery. However, the integration of IoMT devices into healthcare systems presents significant security challenges, particularly in protecting sensitive patient data and ensuring the reliability of medical devices. The diversity of data formats used by various vendors in RPM complicates data aggregation and fusion, thereby hindering overall cybersecurity efforts.

This thesis proposes a novel semantic framework for vulnerability detection in RPM settings within the IoMT system. The framework addresses interoperability, heterogeneity, and integration challenges through meaningful data aggregation. The core of this framework is a domain ontology that captures the semantics of concepts and properties related to the primary security aspects of IoT medical devices. This ontology is supported by a comprehensive ruleset and complex queries over aggregated knowledge. Additionally, the implementation integrates medical device data with the National Vulnerability Database (NVD) via an API, enabling real-time detection of vulnerabilities and improving the security of RPM systems.

By capturing the semantics of medical devices and network components, the proposed semantic model facilitates partial automation in detecting network anomalies and vulnerabilities. A logic-based ruleset enhances the system's robustness and efficiency, while its reasoning capabilities enable the identification of potential vulnerabilities and anomalies in IoMT systems, thereby improving security measures in remote monitoring settings.

The semantic framework also supports knowledge graph visualization and efficient querying through SPARQL. The knowledge graph provides a structured representation of interconnected data and stores Cyber Threat Intelligence (CTI) to enhance data integration, visualization, and semantic enrichment. The query mechanism enables healthcare providers to extract valuable insights from IoMT data, notifying them about new system vulnerabilities or vulnerable medical devices. This demonstrates the impact of vulnerabilities on cybersecurity requirements (Confidentiality, Integrity, and Availability) and facilitates countermeasures based on severity. Consequently, the framework promotes timely decision-making, enhancing the overall efficiency and effectiveness of IoMT systems. The semantic framework is validated through various use cases and existing frameworks, demonstrating its effectiveness and robustness in vulnerability detection within the domain of IoMT security.

Copyright and access declaration

I certify that this thesis does not, to the best of my knowledge and belief:

- incorporate without acknowledgement any material previously submitted for a degree or diploma in any institution of higher education;
- contain any material previously published or written by another person except where due reference is made in the text of this thesis;
- contain any defamatory material;

Signed:

Date: 16-6-2024

Acknowledgments

First of all, I am thankful to Allah Almighty for enabling me to reach the end of my doctoral dissertation. I praise Him, seek His forgiveness, and ask for His help as He is the greatest benefactor.

I would like to express my heartfelt gratitude to my entire family, including my parents and in-laws. My deepest gratitude goes to my late father, Abdul Karim Unar, whose unwavering support for education inspired me to pursue and reach new milestones in my career. I am deeply thankful to my mother, Fatima Unar, who raised me with love and affection and always motivated me to excel in life. I am grateful to my brothers, Abdul Saleem, Abdul Hameed, and Abdul Majeed, as well as my sisters for their constant moral support and help, which strengthened me during challenging times.

A special thank you goes to my beloved husband, Muhammad Aneel Bughio, who stood by me through both good and bad times. During this long and difficult journey, Aneel was a great source of strength, constantly encouraging me to persist and complete my PhD. Very special thanks to my son, Sindhyar, and my daughter, Aizel. Their love always made me strong and motivated me to reach my goal. Without their patience, I could not have completed this journey. Their sacrifices will never be forgotten.

I would like to extend my sincere thanks and highest regards to my supervisor, Dr. David Michael Cook, for his constant support, invaluable help, and exceptional mentorship for my PhD completion. His timely guidance and constant motivation were crucial to my success. I also wish to express my sincere gratitude to my associate supervisor, Dr. Syed Afaq Ali Shah, whose consistent support, insightful feedback, and expert guidance were instrumental in navigating the challenges of my research.

I acknowledge and thank Dr. Naeem Janjua, Dr. Syed Shamsul Islam from Edith Cowan University, and Dana Dermody from the University of the Sunshine Coast, Queensland, for their support and valuable feedback during my PhD studies. I thank you all for being my supervisors during this memorable journey.

I acknowledge and thank my all friends and lab fellows for their support and help, which enabled me to excel in my studies. The support and assistance from my colleagues in Lab 18.420 will always hold a special place in my memories.

I extend my sincere thanks to the School of Science and Graduate Research Services (GRS) at Edith Cowan University (ECU) for providing all the necessary support whenever I needed it.

Last but not least, I would like to extend my gratitude to Edith Cowan University (ECU) in Australia and the Higher Education Commission (HEC) of Pakistan for providing me with funding.

List of Publications

The following is a list of publications (Published or accepted) that have resulted from the research conducted in this thesis.

- Bughio, K. S., Cook, D.M., Shah, A., "Investigating the intersections of vulnerability detection and IoMTs in healthcare, a scoping review protocol for Remote Patient Monitoring". Research, Society and Development, 2024, Volume 13, No. 6. https://rsdjournal.org/index.php/rsd/article/view/46080. ***(Chapter 2)***.

- Kulsoom S. Bughio and L. F. Sikos, Knowledge Organization Systems to Support Cyber-Resilience in Medical Smart Home Environments. Springer International Publishing, 2023. https://doi.org/10.1007/978-3-031-24946-4_5. ***(Chapter 2)***.

- Bughio, K.S.; Cook, D.M.; Shah, S.A.A., "Developing a Novel Ontology for Cybersecurity in Internet of Medical Things-Enabled Remote Patient Monitoring". Sensors 2024, 24, 2804. https://doi.org/10.3390/s24092804. ***(Chapter 4)***

- Kulsoom S. Bughio, "Knowledge Organization System for Partial Automation to Improve the Security Posture of IoMT Networks." Procedia Comput Sci, vol. 225, pp. 3471–3478, 2023, https://doi.org/10.1016/j.procs.2023.10.342. ***(Chapter 5)***.

- Bughio, K.S., Cook, D.M., Shah, S.A.A. (2024). Novel Knowledge Graph-Based Modeling for Vulnerability Detection in the Internet of Medical Things. In: Nguyen, N.T., et al. Recent Challenges in Intelligent Information and Database Systems. ACIIDS 2024. Communications in Computer and Information Science, vol 2144. Springer, Singapore. https://doi.org/10.1007/978-981-97-5937-8_26 ***(Chapter 6)***.

- Bughio, K. S., Cook, D.M., Shah, S.A.A., "Generative AI Models in Rule-Based Systems: Testing and Evaluation". **Accepted** in 28th Annual KES Conference Seville, Spain 11-13 September 2024. http://kes2024.kesinternational.org/ ***(Chapter 7)***.

The following is a list of publications currently under review or in the process of publication:

- Bughio, K. S., Cook, D.M., Shah, S.A.A., "Challenges and Solutions in Securing Medical IoT Systems". International Journal of Information Security. pp: 1-11. ***(Chapter 1)***.

- Bughio, K. S., Cook, D.M., Shah, S.A.A., "IoMT Security: A Semantic Framework for Vulnerability Detection in Remote Patient Monitoring. International Journal of Information Management. 2024. ***(Chapter 7 and Chapter 8)***.

Contents

Contents vii

List of Figures xii

List of Tables xvi

List of Important Terms xviii

List of Abbreviations xxii

List of Variables and Symbols xxiv

Conventions xxiv

1 Introduction 1

1.1 Background 1

1.1.1 The Rise of IoT in Healthcare and its Security Concerns 2

1.2 Problem Statement 6

1.2.1 Research Challenges 7

1.2.1.1 Modelling challenges 7

1.2.1.2 Processing challenges 8

1.2.1.3 Visualization challenges 9

1.3 Research Questions 10

1.4 Aims and Objectives of the Study 10

1.5 Significance of the Study 12

1.6 Scope of the Study 13

1.7 Contributions of the Research 13

1.8 Organization of the Thesis 14

1.8.1 Chapter 2: Literature Review and Background 15

1.8.2 Chapter 3: Research Methodology and Research Design 15

1.8.3 Chapter 4: Developing a Novel Ontology for Cybersecurity in Internet of Medical Things-Enabled Remote Patient Monitoring 15

1.8.4 Chapter 5: Knowledge Organization System for Partial Automation to Improve the Security Posture of IoMT Networks 16

1.8.5 Chapter 6: Novel Knowledge Graph-Based Modeling for Vulnerability Detection in the Internet of Medical Things . . . 16
1.8.6 Chapter 7: Implementation, Testing and Validation . . . 16
1.8.7 Chapter 8: Results and Findings . . . 16
1.8.8 Chapter 9: Conclusion and Future Work . . . 16
1.9 Summary of the Chapter . . . 17

2 Literature Review and Background 18
2.1 Internet of Medical Things (IoMT) . . . 18
2.1.1 Remote Patient Monitoring Systems . . . 21
2.2 Medical Device Categorization . . . 23
2.2.1 Common Medical Devices based on Usage and Placement . . . 23
2.2.2 Common Medical Devices based on functionality . . . 25
2.3 Cyber-Resilience for IoMT is an Interdisciplinary Research . . . 26
2.3.1 Cyberattacks in Real-time Healthcare Applications . . . 26
2.3.1.1 Cyberattacks on Medical Devices . . . 27
2.3.1.2 Cyberattacks in Hospitals . . . 27
2.3.1.3 Cyberattacks in Aged Care Facilities . . . 29
2.3.2 The Role of Legislation and Standards for Cyber-Resilience in Medical Smart Homes . . . 29
2.3.3 Knowledge Organization Systems for Cyber-Resilience in Medical Smart Home Environments . . . 31
2.3.3.1 Semantic models for IoMT . . . 32
2.3.3.2 Cybersecurity Solutions for IoMT . . . 34
2.3.4 Information Security Countermeasures in Medical Smart Homes . . . 34
2.4 Key Technologies and Tools in Semantic Framework Development . . . 35
2.4.1 Ontology Development . . . 35
2.4.1.1 Tools for Developing Ontologies . . . 36
2.4.1.2 Reasoning Mechanism . . . 38
2.4.1.3 Generative Artificial Intelligence (Gen AI) . . . 40
2.4.1.4 Knowledge Graph . . . 40
2.4.1.5 NVD, CVE and CVSS . . . 41
2.5 Conducting a Scoping Literature Review . . . 43
2.5.1 Vulnerability Detection for IoMT in Remote Patient Monitoring: A Scoping Review . . . 43
2.5.1.1 Summary of Scoping Review . . . 44
2.5.2 Scoping Review Method . . . 44
2.5.2.1 Eligibility Criteria and Sources . . . 44
2.5.2.2 Identifying the research question . . . 44
2.5.2.3 Databases and search strategy for review . . . 45
2.5.3 Study Selection . . . 47

2.5.3.1 Inclusion Criteria . . . 47
2.5.3.2 Exclusion Criteria . . . 48
2.5.4 Data Extraction . . . 48
2.5.5 Results . . . 49
2.5.5.1 General Overview . . . 49
2.5.5.2 Vulnerability and cyberattack detection in IoMT . . . 52
2.5.6 Discussion . . . 64
2.5.6.1 Key Findings . . . 64
2.5.6.2 Limitations . . . 65
2.5.7 Research Gaps and Priorities . . . 65
2.5.8 Conclusion for Scoping Review . . . 67
2.6 Summary of Chapter . . . 67

3 Research Methodology and Design 68
3.1 Research Methodology and Design . . . 68
3.2 Research Phases . . . 69
3.2.1 Problem Formalization . . . 69
3.2.2 Research Phase 2: Proposed Solution . . . 70
3.2.2.1 Phase I- Conceptual Model . . . 72
3.2.2.2 Phase II- Prototype Development . . . 72
3.2.2.3 Semantic Framework . . . 73
3.2.2.4 Evaluation and Validation . . . 73
3.3 Summary of the Chapter . . . 73

4 Developing a Novel Ontology for Cybersecurity in Internet of... 74
4.1 Introduction . . . 75
4.1.1 The Need for a Cybersecurity Ontology for Remote Patient Monitoring . . . 75
4.1.2 The Role of Semantic Models in the Internet of Medical Things . . . 76
4.2 Related Work . . . 77
4.3 Ontological Technology . . . 79
4.4 A Proposed Methodology for Ontology Development . . . 81
4.4.1 Specification and Scope . . . 82
4.4.1.1 Data Acquisition . . . 82
4.4.1.2 Competency Questions . . . 83
4.4.1.3 Answers to the Competency Questions . . . 83
4.4.2 Reusing Existing Ontologies . . . 84
4.4.3 The Term Enumeration . . . 84
4.4.4 Conceptualization . . . 84
4.4.4.1 Data Dictionary . . . 85
4.4.4.2 Concepts Classification Tree . . . 86
4.4.4.3 Table of Object Properties and Table of Data Properties . . . 87

4.4.4.4 Table of Instances . . . 89
4.4.5 Formal Grounding with Description Logics . . . 90
4.4.5.1 Concepts Hierarchy in Description Logic . . . 90
4.4.5.2 Role Definition in Description Logic . . . 92
4.4.5.3 Individual Declarations . . . 93
4.5 Developing the Conceptual Model for MIoT Ontology . . . 93
4.5.1 Detailed Description of MIoT Model . . . 93
4.5.2 Case Study . . . 95
4.5.2.1 Assumptions . . . 96
4.5.3 Evaluation . . . 96
4.6 Limitations and Future Work . . . 98
4.7 Conclusions . . . 98

5 Knowledge Organization System for Partial Automation to ... 100
5.1 Introduction . . . 100
5.2 Related Work . . . 102
5.3 A Proposed MIoT Ontology . . . 102
5.3.1 Specification and Scope . . . 102
5.3.2 Conceptualization . . . 103
5.3.3 Implementation . . . 104
5.3.4 Ruleset . . . 105
5.3.5 Evaluation . . . 106
5.4 Conclusion . . . 108

6 Novel Knowledge Graph-Based Modeling for Vulnerability ... 109
6.1 Introduction . . . 109
6.2 Related Work . . . 110
6.3 A Proposed Framework for Vulnerability Detection Utilizing Knowledge Graph-Based Modeling . . . 112
6.3.1 Knowledge Acquisition . . . 112
6.3.2 Knowledge Management . . . 113
6.3.2.1 MIoT Ontology . . . 113
6.3.2.2 Reasoning Engine . . . 114
6.3.3 Visualization and Query Interface . . . 115
6.3.3.1 MIoT Knowledge Graph . . . 115
6.3.3.2 Integration with Industry Standards . . . 116
6.3.3.3 Access to the SPARQL Endpoint . . . 116
6.4 Discussion . . . 117
6.5 Conclusion and Future Work . . . 118

7 Implementation, Testing and Validation **119**
7.1 A Semantic Framework for Vulnerability Detection in Remote Patient Monitoring . . 120
7.1.1 Semantic Modelling 121
7.1.1.1 Implementation of MIoT Ontology 122
7.1.1.2 Integration with NVD Database 130
7.1.1.3 Reasoning Mechanism 132
7.1.2 Visualization and Query Interface 150
7.1.2.1 Knowledge Graph Visualization 151
7.1.2.2 SPARQL Endpoint 153
7.1.3 Evaluation of MIoT Semantic Model 161
7.1.3.1 Criteria-based Evaluation 161
7.1.3.2 Generative AI-based Model Evaluation 164
7.1.4 Validation of the MIoT Semantic Framework 175
7.1.4.1 Summary of Key Differences 178
7.2 Summary of the Chapter 179

8 Results and Findings **180**
8.1 Results 180
8.1.1 Implementation of the Semantic Framework 181
8.1.1.1 Semantic Model 181
8.1.1.2 Visualization and Query Interface 182
8.1.2 Comparative Analysis 182
8.2 Findings 183
8.2.1 Significance of major and supporting findings 183
8.2.2 Summary of Findings 183
8.2.3 Key Findings 185
8.3 Limitation and Challenges of Study 187
8.4 Summary of the chapter 188

9 Conclusion and Future work **189**
9.1 Conclusion of the Thesis 189
9.2 Future Work 190

Bibliography **191**

Appendices **213**

A List of Vendors, Products, Medical devices and Tecnology **213**

B Selected Studies for Scoping Review **216**

C Python Script for Integrating CVE Data into MIoT Ontology **226**

List of Figures

1.1 Medibank breached in Dec 2022, affecting 9.7 million People [1]. 3
1.2 Broward Health breaches in January 2022, effecting1.3 million People [2],[3]. 4
1.3 Graphical representation of the number of breaches that occurred in the years 2021 and 2022 from January to June. 4
1.4 Top five sectors to notify data breaches [4] 5
1.5 Sources of data breaches [4] 5

2.1 General architecture for the Internet of Medical Things (IoMT). 19
2.2 Knowledge Organization Systems features adapted from [5], [6], [7] 32
2.3 A sample NVD CVE Json entry. 42
2.4 PRISMA Study Selection Process [8], [9], [10] 50
2.5 Statistics of research articles selected for Scoping Review. 51
2.6 Included Studies by Year of Publication. 51
2.7 Included Studies by Technology used in IoMT for vulnerability/cyberattack detection. 51
2.8 Included Studies by Technology used in IoMT for vulnerability/cyberattack detection. 52

3.1 The Science and Engineering Methodology for Semantic Framework Development. . 70
3.2 Pipeline of activities for the proposed Solution. 72

4.1 Class diagram for the Concept Classification Tree. 87
4.2 The Conceptual model of MIoT ontology. 94
4.3 The granularity of MIoT ontology described for the concept `Product` with subclasses, instances, and relationship. 94

5.1 The hierarchical concepts for MIoT ontology. 105
5.2 The SPARQL Query Result. 107
5.3 The SPARQL Query Result. 107
5.4 The SPARQL Query Result. 108

6.1 A Semantic Framework for Vulnerability Detection based on Knowledge Graph (Source of Images: Google). 113
6.2 The Domain-Range graph for the concept Product. 116

7.1 A Semantic Framework for Vulnerability Detection in Remote Patient Monitoring . . 121

7.2 The relationship of Concept_Product with its subClasses and individuals. 123
7.3 The relationship of Concept_MedicalDevice with its subClasses and individuals. 124
7.4 The Concept_Vulnerability with its subClasses, relationships and individuals. 124
7.5 The Concept_Service with its subClasses, relationships and individuals. 125
7.6 The relationship of Concept_Person with subClasses and individuals. 125
7.7 The relathionship of Concept_Vendor with other classes and individuals. 126
7.8 The relationship of Concept_Attack with its subClasses and individuals. 126
7.9 The Concept_AdverseSideEffect with its neighbour concept and individuals. 127
7.10 The relationship of Concept_Countermeasure with its subClasses and individuals.128
7.11 The Concept_Exploit with neighbour concepts, relationships and individuals. . . 128
7.12 The Concept_MedicalDeviceFunction with neighbour concepts, relationships and individuals. 129
7.13 The Concept_Target with its subClasses, relationships and individuals. 130
7.14 The maxInclusive and minInclusive values for *hasBloodPressure* data property.134
7.15 The maxInclusive and minInclusive values for *hasDosageValue* data property.136
7.16 Reasoning mechanism by Inference Engine. 140
7.17 Ruleset implementation in Protégé desktop application 145
7.18 Rule 1: The inferred axiom shown as "HighBloodPressureReading". 145
7.19 The inferred axiom shown as ”CompromisedMedicalDevice”. 146
7.20 The inferred axiom shown as ”AdverseSideEffect”. 146
7.21 The inferred axiom for DeliverMedication shows the LifeThreatening. . 147
7.22 The inferred axiom shown as ”Exploit”. 147
7.23 The inferred axiom shown as NetworkLayer attacks for ”VulnerabilityCVE-2013-10029” 148
7.24 The inferred axiom shown as hasRiskLevel HigHRisk due to ”high Severity”. . . . 148
7.25 The MitigationRecommendations suggested for VulnerabilityCVE-2021-31233 149
7.26 The InstallSoftwareUpdate inferred axiom shown as MitigationRecommendation. . . 149
7.27 The medical device Pacemaker has MitigationRecommendation is suggested due to HighRisk. 150
7.28 Domain-Range graph for the concept Product 152
7.29 Domain-Range graph for the concept Vulnerability 152
7.30 The individual Pacemaker with CIA information 153
7.31 The individual Pacemaker extended with the information about related entities . . . 153
7.32 MedicalDevice used in IoMT environment. 154
7.33 MedicalDevice along with their Product. 155
7.34 List of Vendor used in IoMT. 155
7.35 MedicalDevice, Product and their Vendor. 156
7.36 MedicalDevice with their OperatingSystem, Protocol and Technology used. 156

7.37 List of vulnerabilities present in IoMT devices 157
7.38 MedicalDevice that are *not vulnerable* 158
7.39 `MedicalDevice` that are *vulnerable* 158
7.40 The `Patient` are effected and cause `AdverseSideEffect`. 159
7.41 `DataType` affected by vulnerabilities and impacts on *CIA*. 159
7.42 Medical devices shows the adverse side effects if these are vulnerable. 160
7.43 `MedicalDevice` and its `AdverseSideEffect` 160
7.44 Consistency checking in Pellet Reasoner 161
7.45 rdfs:comment for Concept `Product` 162
7.46 The hierarchical *Concepts* in MIoT Ontology. 162
7.47 List of *Object Properties* for MIoT Ontology. 162
7.48 List of *Data Properties* for MIoT Ontology. 162
7.49 The Individual `Pacemaker` and related Vulnerabilities 163

List of Algorithms

1 Vulnerability Detection in Medical IoT Devices 71
2 Pseudocode for Python Program NVD JSON File 131

List of Tables

2.1 Population, Concept, and Context (PCC) . . . 44
2.2 Search Strings and Results . . . 46
2.3 Inclusion Criteria . . . 47
2.4 Exclusion Criteria . . . 48

3.1 Solution Methodology Phases . . . 71

4.1 FOL, DL and OWL Terminologies . . . 79
4.2 Abbreviations and Descriptions . . . 80
4.3 Ontology Development Process . . . 82
4.4 Table for Data Dictionary . . . 86
4.5 Table of object properties with their domain and range. . . . 88
4.6 Table of data properties with their domain and range. . . . 89
4.7 Table of instances and their description. . . . 89
4.8 Notations for Concepts and their description used in Scenario X. . . . 97

5.1 List of Object Properties with their Domain and Range . . . 103
5.2 List of Data Properties with their Domain and Range . . . 104

7.1 Prefix Definitions . . . 122
7.2 Steps to Perform Automated Reasoning . . . 133
7.3 Detection of High Blood Pressure Reading . . . 135
7.4 Data Modification due to Vulnerability . . . 135
7.5 Adverse Side Effects occur due to an increase in Medication Dosage . . . 136
7.6 Vulnerability Exposure to Exploit . . . 136
7.7 Vulnerability Considered Vulnerable to Attack . . . 137
7.8 High Risk of Attack for Medical Devices with High Severity . . . 137
7.9 Mitigation Recommendation for Vulnerability . . . 138
7.10 Mitigation Recommendation for Medical Devices with Any Risk Level . . . 138
7.11 SWRL Rules and their Descriptions . . . 143
7.12 Mappings between MIoT Ontology and NVD Database . . . 151
7.13 **Rule 1**: Test Results for HighBloodPressureReading Detection . . . 166
7.14 Confusion Matrix for *Rule 1:* HighBloodPressureReading Detection . . . 166

7.15 **Rule 2:**Test Results for CompromisedMedicalDevice Detection (CMD) 167
7.16 Confusion Matrix for *Rule 2:* CompromisedMedicalDevice Detection 167
7.17 **Rule 3:** Test Results for Adverse Side Effects Detection 168
7.18 Confusion Matrix for *Rule 3:* AdvereSideEffect Detection 168
7.19 **Rule 4:** Test Results for Vulnerability and Exploit Detection 169
7.20 Confusion Matrix for *Rule 4:* Vulnerability and Exploit Detection 169
7.21 **Rule 5:** Test Results for Vulnerability, Exploit, and Attack Detection 170
7.22 Confusion Matrix for Rule 5: Vulnerability, Exploit and Attack Detection 170
7.23 **Rule 6:** Test Results for Medical Device Attack Risk Detection 172
7.24 Confusion Matrix for *Rule 6:* Medical Device Attack Risk detection 172
7.25 **Rule 7:** Test Results for Mitigation Recommendations (MR) 173
7.26 Confusion Matrix for *Rule 7:* Mitigation Recommendation (MR) 173
7.27 **Rule 8:** Test Results for Mitigation Recommendations Based on Risk Levels 174
7.28 Confusion Matrix for *Rule 8:* Mitigation Recommendation (MR) based on Risk Level 174
7.29 Comparison of MIoT Semantic Framework and IoMT-SAF 176

A.1 List of Vendors Providing Medical Devices in Healthcare with Technology 213

B.1 Comparison of studies based on proposed criteria related to Technologies, Area of Research (AoR), Knowledge Organization Systems (KOS), Automated Reasoning (AR), Cyberattacks/Vulnerability Detection (C/VD), and Knowledge Graph Representation (KGR). 216

List of Important Terms

IoMT	IoMT (Internet of Medical Things) is a collection of various medical devices and their applications within the research domain. These devices can collect, transmit, and share patient data and other healthcare information, enabling remote monitoring, diagnosis, treatment, and management of medical conditions [11].
Domain Ontology	A formal representation of knowledge as a set of concepts within a domain and the relationships between those concepts [12].
Ontology Engineering	The process of developing and maintaining ontologies, which includes activities such as conceptualization, formalization, implementation, and evaluation [13].
MIOT Ontology	MIoT ontology or (Medical Internet of Things) ontology are interchangeably terms used in this Thesis. MIoT ontology is a fundamental domain ontology, focusing on cybersecurity in IoMT (Internet of Medical Things), particularly in remote patient monitoring settings. It defines various concepts, roles, and individuals. The MIoT ontology, MIoT Knowledge Graph, and MIoT Semantic Framework are all terms proposed by the researcher of this Thesis.
Medical device	A medical device involves a broad range of instruments, apparatuses, machines, software, implants, or comparable items utilized for medical purposes. These are manufactured to diagnose, treat, monitor, or alleviate medical conditions, diseases, or disabilities in patients [14].
RPM	Remote Patient Monitoring (RPM) involves the use of digital technologies to collect health data from patients in one location and electronically transmit that information securely to healthcare providers in a different location for assessment and recommendations [15].

Semantic Web	The Semantic Web is an extension of the World Wide Web (WWW) that aims to make internet data machine-readable and interpretable by providing a framework that allows data to be shared and reused across different applications, enterprises, and communities [16].
RDF	The Resource Description Framework (RDF) is a framework for representing information about resources in the web. It uses a graph-based model to describe relationships between resources in a structured and machine-readable way. RDF provides a standard way to describe and interlink data, enabling interoperability across different systems [17].
OWL	The Web Ontology Language (OWL) is a formal language used to create and share ontologies on the web. It is designed to represent rich and complex knowledge about things, groups of things, and the relationships between things. OWL is part of the W3C's Semantic Web standards and provides more expressiveness than other languages like RDF Schema.
XSD	XSD serves as a formal description method for specifying the structure and elements within an XML (Extensible Markup Language) document [18].
Automated Reasoning	The use of computers to emulate human reasoning in problem-solving, often used in the context of proving mathematical theorems, validating software, and other applications of artificial intelligence.
Knowledge Graph	A knowledge graph is a structured representation of knowledge in the form of a graph, where nodes represent entities and edges represent relationships between entities. It is used to integrate and reason over diverse data sources.
NVD	The National Vulnerability Database (NVD) is a U.S. government repository of standards-based vulnerability management data.
NIST Cybersecurity Framework	Developed by the National Institute of Standards and Technology (NIST), this framework provides a set of guidelines and best practices for organizations to manage and enhance their cybersecurity posture [19].

MITRE	The MITRE Corporation is a not-for-profit organization that operates federally funded research and development centers (FFRDCs) to support various U.S. government agencies. MITRE conducts research and provides engineering and technical expertise to help solve complex challenges in areas such as defense, cybersecurity, healthcare, and aviation.
CVE	Common Vulnerabilities and Exposures (CVE) is a list of publicly disclosed cybersecurity vulnerabilities and exposures maintained by the MITRE Corporation.
CVSS	The Common Vulnerability Scoring System (CVSS) provides a standardized way to assess the severity of security vulnerabilities.
Health Level Seven (HL7)	HL7 develops international standards for the exchange of electronic health information. The Fast Healthcare Interoperability Resources (FHIR) is a specific HL7 standard gaining prominence in IoMT [20].
Health Insurance Portability and Accountability Act (HIPAA)	HIPAA sets the standard for protecting sensitive patient data. It mandates the implementation of security and privacy measures to safeguard electronic health information [21].
Comprehensive ruleset	A detailed set of rules used to govern, control, or manage a specific process, system, or behavior within a given context.
ALO$^{(D)}$	It is a logical operator used in description logics to specify that there is at least one distinct instance of a given property or class. This operator is often used in formal knowledge representation and reasoning to enforce the existence of at least one unique instance in a particular context.
Complex Queries	Queries that involve multiple criteria, conditions, or operations, often used in database management and information retrieval to extract specific information from large datasets.
Conceptualization	The process of defining and organizing concepts and their relationships within a particular domain, often used as a preliminary step in ontology development.
Cyberthreat Intelligence	Information about threats and threat actors that helps organizations prevent, identify, and respond to cyber attacks.
Generative AI Model	A type of artificial intelligence model that can generate new data instances that resemble the training data, used in various applications such as image creation, text generation, and more.
Data Visualization	The graphical representation of data to help people understand, interpret, and derive insights from complex datasets.

Ruleset Generation	The process of creating a set of rules or guidelines, often for automated decision-making systems, regulatory compliance, or other applications.

List of Abbreviations

ACSC	Australian Cybersecurity Centre
AI	Artificial Intelligence
API	Application Programming Interface
BLE	Bluetooth Low Energy
CCT	Concepts Classification Tree
CIA	Confidentiality, Integrity, Availability
CPE	Common Platform Enumeration
CT	Computed Tomography
CTI	Cyberthreat Intelligence
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DD	Data Dictionary
DL	Description Logic
D (HHS)	Department of Health and Human Services
EHRs	Electronic Health Records
EP	Essential Principles
FOL	First Order Logic
GenAI	Generative AI
GPRS	General Packet Radio Service
HIPAA	Health Insurance Portability and Accountability Act
HL7	Health Level Seven
ICMR	Indian Council of Medical Research
ICN	Information-Centric Networking
ICT	Information and Communication Technologies
IoMT	Internet of Medical Things
IoMT-SAF	Internet of Medical Things Security Assessment Framework
IoT	Internet of Things
JBI	Joanna Briggs Institute
JSON	Javascript Object Notation
KG	Knowledge Graph
KR	Knowledge Representation

KOS	Knowledge Organization System
LAN	Local Area Network
LTE	Long Term Evolution
MID	Medical Imaging Devices
MIoT	Medical Internet of Things
MIT	Massachusetts Institute of Technology
MQTT	Message Queuing Telemetry Transport
MRI	Magnetic Resonance Imaging
NB-IOT	Narrowband Internet of Things
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
OWL	Web Ontology Language
PAN	Personal Area Network
PRISMA	Preferred Reporting Items for Systematic Reviews and Meta-Analyses
RDF	Resource Description Framework
RDFS	RDF Schema
RDF/XML	Resource Description Framework/Extensible Markup Language
RFID	Radio-Frequency Identification
RQ	Research Question
RPM	Remote Patient Monitoring
SLR	Systematic Literature Review
SPARQL	SPARQL Protocol and RDF Query Language
SW	Semantic Web
SWRL	Semantic Web Rule Language
WAN	Wide Area Network
WBAN	Wireless Body Area Network
WSAN	Wireless Sensor and Actuator Networks
XML	Extensible Markup Language
XSD	XML Schema Definition

List of Variables, Symbols, and Conventions

Variables and Symbols

$\sqsubseteq$	Subclass relation
$\top$	Top or universal concept
$\bot$	Bottom
$\exists$	Existential quantification
$\forall$	Universal quantification
$\wedge$	Logical “AND”
$\vee$	Logical “OR”
$\rightarrow$	Logical ”implies” or ”if-then” operator

Conventions

IoMT or medical IoT devices	In this document, the terms ”IoMT” and ”medical IoT” or ”medical IoT devices” are used interchangeably to refer to the domain/area of the research. It contains medical devices, networks, connectivities, etc.
MIoT	In this document, the term ”MIoT” is used in many places only for the proposed ontology, knowledge graph, or semantic framework by the researcher. The term MIoT is not used for the domain or area of research.
Instance or Individual	In this document, the terms ”instance” and ”individual” are used interchangeably to refer to an object in RDF triples. (i.e., RDF Triple: Subject $\rightarrow$ Predicate $\rightarrow$ Object.
Concept or Class	The terms ”concept” and ”class” are used interchangeably to refer to a subject/entity in RDF triples.
Role or Relationship	In this document, the terms ”Role” and ”Relationship” are used interchangeably to refer to a predicate in RDF triples. These are properties that connect concept to concept or concept to individual.

Chapter 1

Introduction

This chapter provides an overview of the Internet of Medical Things (IoMT), highlighting the need to focus on this technology, its significance, and its wide application such as Remote Patient Monitoring. It explores the role of knowledge organization systems in modeling and reasoning for vulnerabilities in IoT medical devices in remote patient settings. Furthermore, this chapter contains the background of the research, identification of research issues, and formulation of the research problem. Based on that research problem and formulated questions, the research objectives of this thesis are developed. Finally, the organization of the thesis is outlined. The contents from this chapter are submitted for publication in a Journal [22].

1.1 Background

Over the last twenty years, there has been a significant advancement in information and communication technologies (ICT) [23] and wireless sensor networks [24], resulting in the creation of real-time healthcare solutions. Such environments are ideal for providing a safe, monitored living space where people can live without intervention, and their health records can be maintained by healthcare providers, who will assist them timely in case of an emergency [25], [26], [27], [28]. The ongoing COVID-19 pandemic has further accelerated the use of these systems, especially for individuals managing chronic medical conditions such as diabetes and cardiovascular diseases. It is predicted that in the coming years, healthcare services for dementia patients [29] and cardiac patients [30] will be further transformed from hospital-based to home-based services by 2030 [31], [32].

As Internet of things (IoT), a term coined by Kevin Ashton in 1999 at MIT [33], technology advances rapidly, healthcare providers can now connect with patients beyond the confines of the clinic and reach those in remote locations. In this context, the Internet of Medical Things (IoMT) has played a pivotal role in connecting patients with healthcare professionals and hospitals. IoMT is a form of IoT and is emerging as a significant technology in modern communication systems [11]. IoMT is a collection of IoT technologies that connect doctors, patients, and healthcare providers by transmitting data over a network. These technologies utilize various medical devices and applications in the healthcare field, such as smartphones, surveillance cameras, wearable sensors, and actuators [11], [34], [35], [36].

In the current era, IoT medical devices play an important role in healthcare, providing patient monitoring, assistance, and diagnosis both locally and remotely. Notable examples include telehealth, telemedicine, eHealth applications, clinical medicine, aged care, and remote patient monitoring. Remote patient monitoring (RPM) allows patients to connect with medical practitioners as needed without having to leave home or wait for their turn at the hospital. This infrastructure enables the continuous transfer of real-time patient information via medical devices connected to IoT sensors.

Medical IoT devices can detect patients' conditions and behavior by monitoring blood pressure, heart rate, and other vital signs. For instance, smart blood glucose monitors are equipped with wireless communication technologies like Bluetooth or Wi-Fi. These devices can continuously monitor the patient's health and transmit the data to a server, typically a cloud server [37]. If any abnormal readings are detected, which could be caused by either system errors or hacking, a doctor or caregiver is alerted [38], [39].

However, with these advancements come new challenges, especially in terms of cybersecurity. Remote monitoring is often vulnerable to security breaches and cyberattacks due to the lack of standardized protocols defined by regulatory bodies and device manufacturers across different devices. This situation makes it difficult to maintain cyber-resilience in terms of data security, scalability, heterogeneity, interoperability, and integration throughout such networks, due to the exposure of data and the various types of networks having different functionalities and specifications [40]. While these systems provide benefits to medical staff and patients, they are prone to security risks. For example, sensitive medical and financial data can be stolen or replaced by attackers. As a result of this patients' health could be compromised.

1.1.1 The Rise of IoT in Healthcare and its Security Concerns

Due to the rapid advancements in IoT, healthcare providers are shifting their services from clinics to patients' homes. Remote patient monitoring systems allow patients to connect with doctors remotely when needed, without travelling too far from home and waiting for their turn at the physician's clinic. Similarly, nowadays, medical devices are more portable, connected through a network and have the capability to provide services to patients remotely. On the other hand, these medical devices face security breaches due to a lack of standard protocols defined by regulatory bodies and manufacturers.The security concerns in healthcare are highlighted by the growing market for the Internet of Medical Things (IoMT), which was estimated to reach $158 billion in 2022, up from $41 billion in 2017 [41].

In October 2023, the Indian Council of Medical Research (ICMR) [1] was involved in an incident that affected 815 million records, affected 815 million records [42].

Apart from that, various healthcare organizations' systems have also affected, including Medibank and Broward Health Care. In December 2022 [1], Medibank, an Australian health insurance company, fell victim to a major data breach affecting approximately 9.7 million people. The attack was linked to a well-known ransomware group based in Russia called REvil. The breach was discovered when REvil posted a folder containing 6GB of raw data samples on their dark web blog. Medibank refused

[1] https://timesofindia.indiatimes.com/india/government-probing-data-breach-of-8-crore-indians-from-icmr-covid-site/articleshow/104835828.cms

to pay the $10 million ransom demanded by the attackers. The compromised data included names, birthdates, medical claims numbers, passport numbers, and medical records as shown in Figure 1.1.

medibank
Date: December 2022
Impact: 9.7 million people
In December 2022, Medibank, the Australian health insurance giant, was the victim of a major data breach, affecting the personal details of 9.7 million customers. The attack was believed to be linked to a well-known ransomware group based in Russia, the REvil ransomware gang.
The privacy breach was first discovered when REvil posted on a dark web blog a folder that contained 6GB of raw data samples, indicating that they had larger amounts of data to release, and demanded a $10 million ransom. The data included:
Names
Birthdates
Passport numbers
Medical claims data
Medical records

Figure 1.1: Medibank breached in Dec 2022, affecting 9.7 million People [1].

Similarly, Figure 1.2 outlines a data breach at Broward Health that occurred in January 2022, affecting approximately 1.3 million patients. The breach was attributed to a compromised third-party medical provider with access to patient data, possibly due to insufficient Multi-Factor Authentication implementation. The compromised patients' information includes names, addresses, dates of birth, driver's license numbers, insurance details, and medical information [2],[3].

In remote patient monitoring, where the health of the patient is the priority, additional factors can impact the performance and security of IoT devices in a network. Accordingly, the chances of cyberattacks and threats are increased, including the following: denial of intended service, update of device functionality, loss of financial data, and privacy and security, amongst others. To ensure secure communication between IoMT, manufacturers provide standards that must be followed as well as protocols defined by regulations. In this way, the interaction between medical devices, sensors, servers, gateways, and applications can be secure if they follow these protocols and standards. The reliability of connectivity must also be ensured by following health industry standards and protocols, as defined by government and industry leadership. For example, the Australian Government Department of Health [43] describes "Standards recognized as suitable to meet regulatory requirements for the cyber security of medical devices, alongside the relevant Essential Principles (EP)". The department lists and defines various EPs for manufacturers of medical devices.

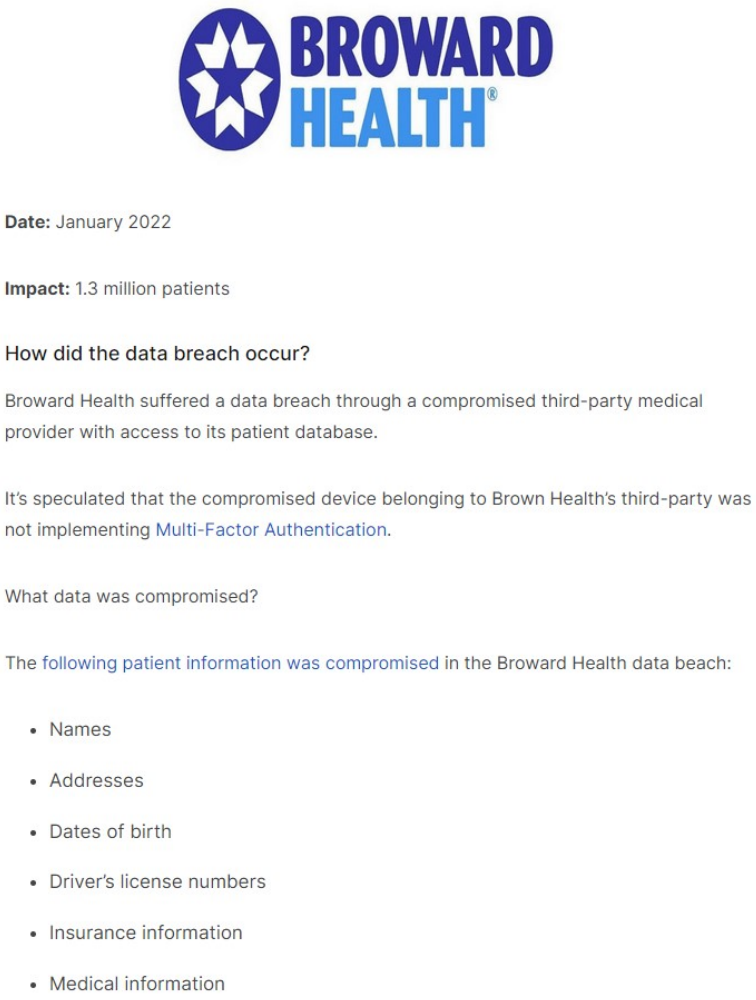
BROWARD HEALTH
Date: January 2022
Impact: 1.3 million patients
How did the data breach occur?
Broward Health suffered a data breach through a compromised third-party medical provider with access to its patient database.
It's speculated that the compromised device belonging to Brown Health's third-party was not implementing Multi-Factor Authentication.
What data was compromised?
The following patient information was compromised in the Broward Health data beach:
Names
Addresses
Dates of birth
Driver's license numbers
Insurance information
Medical information

Figure 1.2: Broward Health breaches in January 2022, effecting1.3 million People [2],[3].

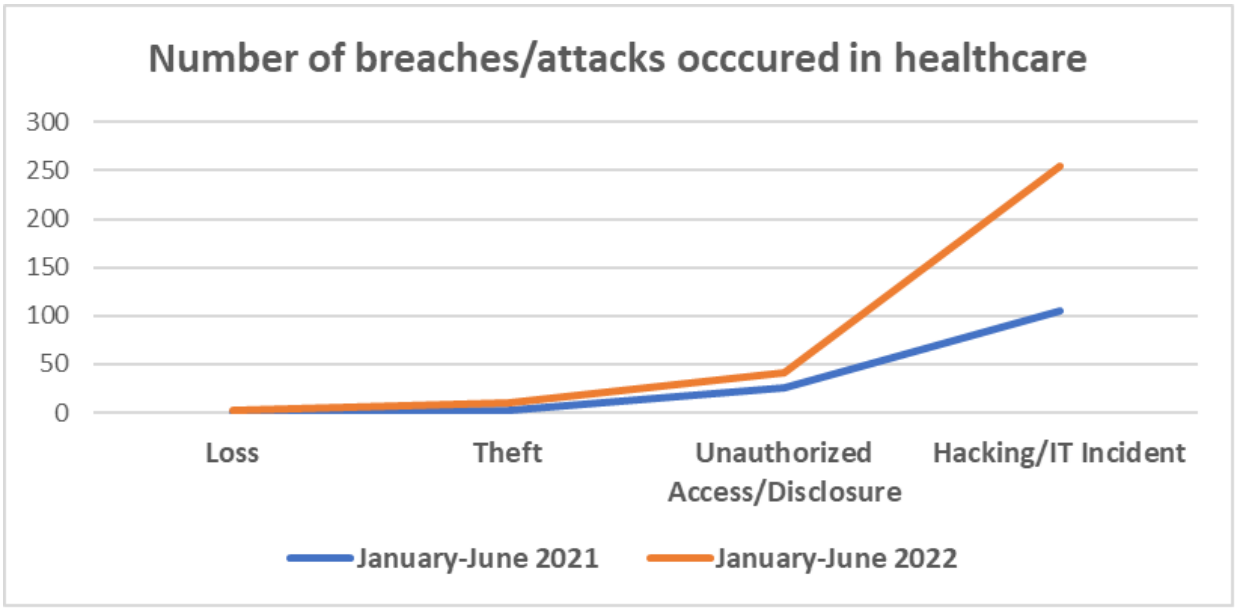

Figure 1.3: Graphical representation of the number of breaches that occurred in the years 2021 and 2022 from January to June.

The U.S. Department of Health and Human Services (HHS) has compiled a record of 125 electronic

data breaches within healthcare organizations for the year 2022. The data reveals a significant increase, with the number of breaches in the first half of the year nearly doubling compared to the same period in the previous year [44], as shown in Figure 1.3.

Similarly for the same period, January-June in the year 2023, according to the report by the Australian government the health sector reported 63 breaches. Most of these breaches (70%) were due to malicious or criminal attacks. The report emphasizes the ongoing challenge of protecting personal information in healthcare, underscoring the need for robust security measures and timely response strategies as shown in Figures 1.4 and Figure 1.5.

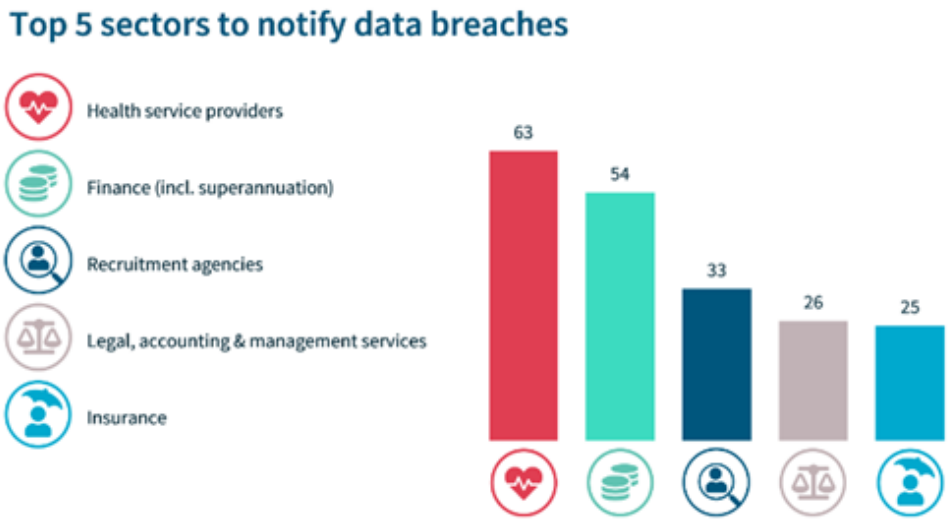

Figure 1.4: Top five sectors to notify data breaches [4] .

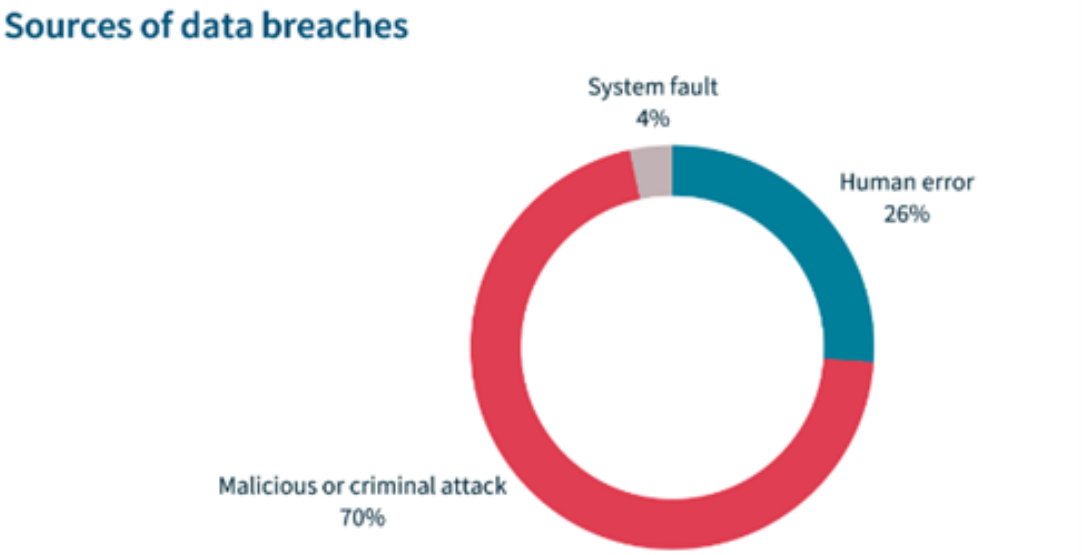

Figure 1.5: Sources of data breaches [4] .

Subsequently, the trend continued with 145 incidents reported in healthcare during the initial three months of 2023 [45]. A recent report from The Health Insurance Portability and Accountability Act of

1996 (HIPAA), published in March 2023, underscores a troubling pattern of data breaches impacting over 4 million patients in total [45], [46].

Furthermore, the Australian Cybersecurity Centre (ACSC) [2] and the Australian Signals Directorate (ASD) responded to 143 cybersecurity incidents related to critical infrastructure such as the health sector in the year 2022-2023 [45] in comparison with 2019 when only 90 cases were reported [46]. According to the HIPAA Journal reported on 15 March 2023 [43], more than 4 million patients' data is compromised in terms of financial accounts, security numbers and medical treatment. According to ACSC, hospitals and aged care are the main targets for cybercriminals. Due to the COVID-19 pandemic, there is a significant increase in healthcare of malicious cyber activities using Maze[3] ransomware on healthcare. In this regard, the ACSC provides guidelines for protection against ransomware, such as backing up files, using patching software, installing antivirus programs, and checking for updates [47].

Given the above, medical IoT devices are well suited for patient monitoring and diagnosis because they can collect, transfer, and interact with (near-) real-time data [36]. Thus, whilst remote monitoring is considered a genuinely advantageous strategy for assisting individuals without the need to transfer to a clinic or hospital, they remain the subject of cyber-strategies to ensure the security of Medical IoT in less-than-ideal environments. Moreover, patient data is transferred through wireless communication, data replacement, data updating, and/or data breaches can be major risks in these systems.

1.2 Problem Statement

Nowadays, IoT devices play an important role in healthcare by monitoring, assisting, and diagnosing patients both locally and remotely. These devices offer significant benefits to medical staff and patients by enhancing care delivery and operational efficiency. However, they also introduce substantial security risks, as sensitive medical and financial data can be targeted by cyber attackers for theft or manipulation.

The management of such systems requires 24/7/365 monitoring and partial automation to maintain security. The diverse data formats used by various vendors' products in medical smart homes present a significant challenge, as they cannot be directly utilized by software agents for data aggregation and fusion. This limitation hinders the support of a robust cybersecurity posture.

Addressing this issue involves capturing the semantics of the components within IoT networks used in these settings. By understanding these semantics, automated reasoning can be employed to detect network anomalies, vulnerabilities, and cyberattacks. This approach enables the automatic identification and response to security threats.

Based on this primary research problem, several key research challenges and issues are identified and discussed here, aiming to enhance the security and functionality of IoT devices in healthcare.

[2] https://www.cyber.gov.au/acsc/view-all-content/advisories/2020-013-ransomware-targeting-australian-aged-care-and-healthcare-sectors

[3] https://www.datto.com/au/blog/what-is-maze-ransomware-and-how-does-it-work

1.2.1 Research Challenges

Despite the advantages of IoMT for healthcare, including enhanced patient monitoring, improved diagnostic capabilities, and more efficient data collection, it faces many issues that are highlighted here. These challenges encompass a broad spectrum of technical, security, and operational concerns that must be meticulously addressed to fully leverage the potential of IoMT technologies in medical settings. The complexities involve not only ensuring the interoperability and integration of diverse IoT devices but also maintaining robust security measures to protect sensitive medical and personal data from sophisticated cyber threats. Additionally, the lack of standardized protocols and the prevalence of proprietary systems further complicate the deployment and management of IoMT infrastructures, often leading to inefficiencies and increased vulnerabilities. The necessity for continuous monitoring, comprehensive semantic modeling, and the establishment of specialized rulesets to handle real-time data further underscore the intricate nature of these challenges. Addressing these multifaceted issues is crucial for advancing the safe and effective use of IoMT in healthcare.

1.2.1.1 Modelling challenges

- *Unavailability of knowledge organisation systems to model the technical and security aspects of IoMT systems*

  With the advancement of technology and highly competitive solutions in IoT in the current era of Industry 4.0, this has created challenges in terms of security, interoperability, privacy, and integration of systems. Rapid alteration in IoT applications can create challenging cyber threats and vulnerabilities in knowledge organization systems. Only a few systems can operate in IoMT to model it in terms of security. In the case of medical devices, when any cyber-attack (i.e., ransomware or phishing) occurs, an organizational system may not have any technical planning to improve cyber resilience.

  With the advancement in technology and highly competitive solutions in IoT in the current era of Industry 4.0, facing challenges in terms of security, interoperability, privacy and integration of systems. The rapid alteration in IoT applications makes it challenging for cyber threats and vulnerabilities in knowledge organization systems. Very few systems can work in IoMT to model it in terms of security. In the case of medical devices, when any cyber-attack (i.e. ransomware or phishing) has occurred, the organisation system has no semantic knowledge to improve cyber resilience.

- *Lack of standardization, proprietary solutions with no publicly available technical specification sufficiently detailed for capturing semantics*

  Due to inappropriate proprietary solutions and standards, the IoMT healthcare infrastructure is regularly at risk. The major challenges faced by IoMT are the lack of standardization and proprietary solutions, with no publicly available technical specifications sufficiently detailed for capturing semantics. In the IoMT infrastructure, various types of medical and non-medical devices are used by different vendors. This in turn can lead to a higher risk of security and

the need to adopt standardization to protect from hacking. Standards and regulations defined by authorized bodies must be applied by organizations to secure their network. However, it is very challenging to adopt the same protocols for all devices to manage security and capture the semantics for a detailed understanding of the system.

- *Unawareness about highly customized IoMT smart home settings*

  The smart home is defined as a collection of electronic devices, sensors, equipment, and wired and wireless communication. This complicated infrastructure requires a setting where each entity is properly and securely connected with the other. However, the IoMT smart home also faces many challenges due to a range of different factors. The users who are involved in this system, such as patients, doctors or other healthcare providers are mostly unaware of the system's configuration and its standards and protocols. They usually have very limited interaction with the devices and are often unaware of any security concerns. Further, vendors and manufacturers who develop the devices do not usually explain the device features, limitations, and cyber resilience in the case of any attack. It is thus necessary to build a customized IoMT smart home setting, where all entities are fully secured such as devices, equipment, and connections. The people involved in this setting should also be well-trained and familiar with technologies and devices.

- *Emerging threats related to IoMT smart home devices and technologies*

  The Internet of Medical Things (IoMT) and smart home technologies are revolutionizing healthcare by enabling remote monitoring, personalized care, and improved patient outcomes. However, these advancements bring with them a range of emerging cyber threats that can significantly impact industries, individuals, and the technologies used in smart home healthcare applications. One of the most prominent and concerning threats is ransomware, which has seen a marked increase in prevalence, particularly in the US and UK.

  The integration of IoMT devices and smart home technologies into healthcare systems introduces new vulnerabilities that can be exploited by cybercriminals. Ransomware attacks, in particular, pose a severe risk by targeting the financial and personal data of patients and healthcare institutions. These attacks can encrypt critical health data, rendering it inaccessible until a ransom is paid. In addition to financial losses and data breaches, these threats can lead to compromised patient health, delayed medical responses, and loss of trust in healthcare technologies. This not only disrupts healthcare services but also puts patients' lives at risk.

1.2.1.2 Processing challenges

- *Lack of specialized ruleset*

  The IoMT infrastructure is made up of various IoT sensors, devices, and technologies. These sensors provide information to the system according to a set of rules. There is a lack of specialized rules for the semantic modelling of those IoT devices. Commonly, SWRL (Semantic Web Rule Language) is used to model the semantics of real-time systems, such as those in

healthcare, involving a combination of OWL with Rule Markup Language. However, this has some limitations for handling complex rules. Thus, there is a need to establish a specialized ruleset that supports the model semantics of IoMT in the real-time scenario.

- *Data Integration and Interoperability*

  Real-time data processing is critical, such as in emergency response or intensive care units. The inability to integrate and interpret data rapidly from multiple sources can impede timely decision-making and negatively impact patient care. The diversity of data types, ranging from simple sensor readings to complex imaging data, adds to the complexity of achieving efficient data integration and interoperability. To address this challenge, there is a need to develop robust methods and standards that ensure compatibility and seamless communication across various IoMT devices and systems. This would involve not only technical solutions but also policy and regulatory efforts to establish and enforce relevant standards. Ensuring data integration and interoperability in IoMT will enhance the system's efficiency, improve patient outcomes, and offer the way for more advanced healthcare analytics and decision-making tools.

1.2.1.3 Visualization challenges

- *Scalability of semantic knowledge graph of real-world IoMT smart home environment*

  IoMT smart homes are designed to cater to specific environments or individuals. For instance, IoMT systems for remote patient monitoring enable patients to use IoT devices comfortably from their homes. Healthcare providers, such as doctors or nurses, can consult patients through internet-based medical devices using Wi-Fi or cloud-based systems. However, these home-based systems are often not efficient for indoor patients or those in hospitals or medical centers due to the specific nature of device configurations and IoT services tailored for home use.

  Another example is aged-care smart homes, where elderly activities are monitored using IoT devices. In these systems, patients can interact with doctors and hospitals, and caregivers can send information to healthcare providers. These setups involve various IoT devices, sensors, and cloud storage. However, they often lack the scalability to provide data for other environments, such as hospital settings. To achieve scalability, it is necessary to provide semantic knowledge of these systems so that they can share their information across different environments.

  Semantically rich information can be highly useful for hospitals to understand and utilize data coming from home-based or aged-care environments, especially in emergencies. By creating scalable semantic knowledge graphs, these IoMT systems can seamlessly integrate and share information with hospital-based systems, ensuring continuity of care and enhancing the overall healthcare ecosystem.

1.3 Research Questions

RQ1: How can data be optimized to support the cybersecurity posture of Remote Patient Monitoring Systems on the Internet of Medical Things (IoMT)?

RQ2: How can vulnerabilities be detected automatically within remote patient monitoring systems?

1.4 Aims and Objectives of the Study

The main aim of this research is to create a semantic framework to facilitate partial automation in improving the security posture of IoT networks used in remote patient monitoring (RPM). At the heart of this framework is a domain ontology that captures the semantics of the concepts and properties related to the primary security aspects of IoT devices used in such systems. This will be complemented by a comprehensive ruleset, complex queries, and a mechanism to enable automated reasoning over the aggregated knowledge. To accomplish this goal, this study divided the main objective into the following sub-objectives:

1. Literature Review and Data Collection **(discussed in *Chapter 2*)**

    - Complete a literature review on knowledge organization systems developed for cybersecurity and IoMT networks in general, specifically focusing on healthcare applications related to remote patient monitoring.
    - Conduct a horizon scan on IoT devices used in remote patient monitoring and gather their technical specifications.
    - To get knowledge about various cybersecurity aspects of medical devices and their applications.
    - To conduct the scoping review to find the research gap, discuss the priority areas of research etc.

2. Ontology engineering

a. Specification **(discussed in *Chapter 4*)**

    - Set the scope of the knowledge organization system, participants used in the ontology, and the purpose of the ontology.
    - Develop an ontology that captures the semantics of concepts and properties for IoT medical devices in remote patient monitoring systems.

b. Data Acquisition **(discussed in *Chapter 4*)**

    - Collect data from expert knowledge, literature, reports, etc., on the security considerations and measures of IT infrastructures used in the healthcare domain.

c. Conceptualization **(discussed in *Chapter 4*)**

- Design an ontology based on background knowledge.
- Define classes, properties, individuals, and their relationships in a machine-interpretable form.

d. Assessment of Potential Term Reuse **(discussed in *Chapter 4*)**

e. Term Enumeration **(discussed in *Chapter 4*)**

f. Formal Grounding with Description Logic Axioms **(discussed in *Chapter 4*)**

i. Concept Hierarchy

ii. Role Definitions

iii. Individual Declarations

g. Ruleset Creation: **(discussed in *Chapter 4, 5, 6 and 7*)**

- Extend the domain ontology with rules to model and reason with cyberattacks and vulnerabilities, such as network layer attacks in healthcare.

h. Implementation (OWL, RDF, SWRL, etc.) **(discussed in *Chapter 5,6 and 7*)**

i. Evaluation via Ontology Engineering Practices and Generative AI Model **(Provided in *Chapter 6)***

3. Automated Reasoning **(discussed in *Chapter 5,6 and 7*)**

- Automated reasoning could be used to analyze security-related data, such as cyber threat intelligence or network activity, to detect anomalies, vulnerabilities or security threats in IoT networks used for remote patient monitoring.

4. Creation of Knowledge Graph, Data Visualization, and Query Retrieval **(discussed in *Chapter 6 and 7*)**

- Generate a knowledge graph to store Cyber Threat Intelligence (CTI) about various medical IoT device networks used in remote patient monitoring.
- Integration with industry-standard vulnerability datasets such as NVD via API for real-time data.
- Queries will performed to interact with data and extract meaningful information in terms of vulnerabilities, their impact and severity.

5. Validation **(discussed in *Chapter 4 and 7*)**

- Validate the proposed framework with existing frameworks/models and use cases in IoMT/remote patient monitoring to detect vulnerabilities.

1.5 Significance of the Study

In several domains, including smart homes and healthcare, IoT devices play a crucial role in monitoring, assisting, and diagnosing patients both locally and remotely. Researchers in healthcare extensively use real-time information systems where IoT, medical devices, various sensors, and cloud services work collaboratively to benefit patients, providing support from their families and remote medical assistance. Monitoring people's health activities with the help of wearable/medical devices is essential. Detecting and preventing cyber-attacks in remote patient monitoring systems (RPMS) is critical to ensure patient safety, protect patient privacy, maintain compliance, and preserve the reputation of healthcare organizations.

The adoption of Remote Patient Monitoring (RPM) empowered by the Internet of Things (IoT) is profoundly significant in healthcare, offering enhanced ease and efficiency across various aspects. These include cost-effectiveness, accessibility, visibility, reliability, accuracy, affordability, continuity of care, and real-time monitoring. For instance, hospitalizing patients incurs substantial costs for patients, healthcare facilities, and insurers. Additionally, individuals residing in remote regions often face challenges in accessing healthcare facilities and caregiver centers, necessitating long-distance travel for medical attention. By integrating IoT into RPM, healthcare systems gain interoperability, streamlined communication, efficient information exchange, and seamless data transfer, thereby elevating the quality of healthcare services. Furthermore, RPM facilitates continuous monitoring of chronic conditions such as diabetes, contributing to proactive management and improved patient outcomes.

From a research perspective, this study focuses on medical IoT devices in RPM. Knowledge organization systems, such as ontologies, play a crucial role in capturing the semantic information of medical IoT devices. Semantic modeling and ontologies provide a logic-based environment of technologies and tools designed to interpret and define knowledge from large, diverse, and unstructured data sources.

The purpose of this research is to create a semantic framework to enhance knowledge in the domain. At the heart of this framework is a domain ontology that represents knowledge through the relationships of concepts based on formal groundings. Rule sets are generated to perform automated reasoning to detect vulnerabilities and cyberattacks in IoMT infrastructure. With automated reasoning, this framework can inform doctors and patients about attacks caused by vulnerabilities, providing significant benefits.

Moreover, integrating vulnerability detection into remote patient monitoring systems serves as a cornerstone for continuous improvement and innovation in healthcare delivery. By constantly monitoring for vulnerabilities and preemptively addressing them through automated reasoning, healthcare organizations can stay ahead of potential security breaches and maintain the resilience of their remote care infrastructure. This proactive stance mitigates the risk of data breaches and cyberattacks and promotes vigilance and responsiveness to evolving cybersecurity threats within the healthcare sector. Ultimately, incorporating vulnerability detection mechanisms not only elevates the security standards of remote patient monitoring but also fosters a safer and more secure environment for both patients

and healthcare providers, laying the foundation for the continued advancement of remote healthcare technologies.

Additionally, the data is stored in a knowledge graph for visualization and querying. This framework will significantly improve the security posture of IoT networks used in remote patient monitoring systems.

1.6 Scope of the Study

The scope of this study encompasses the development and implementation of a semantic framework tailored specifically for medical IoT devices used in remote patient monitoring systems (RPMS). This framework aims to capture and organize semantic information related to these devices, enhancing the security posture of IoT networks within healthcare settings. The study will focus on performing automated reasoning on this semantic framework to detect and prevent cyber-attacks, thereby ensuring patient safety, privacy, regulatory compliance, and the reputation of healthcare organizations. Additionally, the framework will benefit healthcare professionals and patients by generating alerts in case of any detected vulnerabilities or attacks, facilitating timely intervention and mitigation measures.

Automated reasoning finds application in analyzing the functionality of medical devices and detecting potential security flaws. Through the modelling of device behaviour and the application of logical rules, automated reasoning can flag anomalies or deviations from expected behaviour, signalling possible security vulnerabilities. This proactive approach aids in the early identification and mitigation of vulnerabilities, preempting potential exploitation by malicious actors.

To develop a semantic framework centred around a domain ontology that encapsulates the concepts and relationships within the healthcare sector, specifically focusing on the Internet of Medical Things (IoMT) and cybersecurity. This ontology meticulously details and contextualizes the semantics of healthcare and cybersecurity, serving as a crucial tool for vulnerability detection in IoMT environments.

This endeavour required me to communicate complex technical details effectively to diverse audiences. To technical audiences, I presented the underlying structure and technical mechanisms of the ontology through academic conferences, research papers, and collaborative projects, focusing on the technical robustness and application-specific advantages of the framework. For non-technical stakeholders, including healthcare professionals and administrative staff, I simplified the explanations by emphasizing the practical benefits, such as enhanced data security and improved patient care, without delving deeply into the technical complexities. This dual approach ensured that all stakeholders, regardless of their technical background, could appreciate the significance and impact of the research. These experiences have refined my ability to adapt my communication style according to the audience's expertise, facilitating effective sharing and application of my research findings.

1.7 Contributions of the Research

The existing literature in healthcare and cybersecurity identifies a significant research gap concerning the absence of a comprehensive ontology for understanding vulnerabilities in medical (IoT) devices.

To address this gap, this research aims to develop a novel MIoT ontology that incorporates semantics, providing a practical solution. This will involve creating a knowledge graph capable of storing Cyberthreat intelligence. While existing systems typically detect anomalies or cyberattacks using blockchain or IDS systems, the proposed ontology will facilitate automated reasoning through rule-based reasoning, enhancing vulnerability detection in Medical IoT devices. The performance of rule-based reasoning has been analyzed using a Generative AI model, serving as a real-world test for the semantic framework's effectiveness in handling diverse situations. The following are the main contributions of this research work:

1. MIoT ontology- captures the semantics of IoMT, Cybersecurity and Remote Patient Monitoring (RPM) System

   The existing literature in the fields of healthcare and cybersecurity highlights a substantial research gap, specifically the absence of a comprehensive ontology that can effectively offer knowledge regarding vulnerabilities in medical (IoT) devices. In response, this research endeavours to introduce a novel MIoT ontology that not only addresses this gap but also provides a practical solution by incorporating semantics. This will be accomplished through the creation of a knowledge graph capable of storing Cyberthreat intelligence. The rules are generated to perform automated reasoning.

2. Automated Reasoning is performed based on Ruleset contains entities (medical devices, persons, vulnerabilities), and their relationships.

   In the literature, most of the systems detect anomalies/cyberattacks by using blockchain or IDS systems. The proposed ontology will enable automated reasoning with the help of rule-based reasoning, thereby facilitating the detection of vulnerabilities in Medical IoT devices.

3. The proposed semantic model is evaluated using the Generative AI model.

   The proposed model has been analyzed using generative AI to evaluate the performance of rule-based reasoning. This process is akin to evaluating the performance of the Semantic model in real-world scenarios, challenging it to see if it can successfully handle various situations.

4. The Knowledge Graph Visualization and querying.

   The proposed semantic framework leverages knowledge graph visualization, where data triples are converted into nodes and edges, offering a clear and intuitive representation of the system. This visualization aids in understanding complex relationships and structures within the IoMT ecosystem. Additionally, querying capabilities allow users to extract valuable insights from the semantic framework, enabling detailed analysis and informed decision-making.

1.8 Organization of the Thesis

The thesis entirely presents a single body of research. It is s divided into eight chapters. Each chapter contains an introduction and a summary that validates its existence within the thesis.

1.8.1 Chapter 2: Literature Review and Background

This chapter organizes a thorough critical literature review and technological background, building upon the foundational research areas introduced in Chapter 1. It focuses on knowledge organization systems developed for cybersecurity and communication networks, with a special emphasis on healthcare applications, particularly those related to remote patient monitoring. The chapter includes a detailed horizon scan of IoT devices used in remote patient monitoring, analyzing their technical specifications. This involves a close examination of the types of sensor data these devices capture, as well as the standards and protocols prevalent in this domain.

In addition to this comprehensive review, the chapter employs the Joanna Briggs Institute (JBI) methodology to conduct a scoping review. This methodical approach systematically examines the literature to identify existing gaps and pinpoint key issues relevant to the field. Alongside this, the chapter delves into the technical methods and approaches utilized in this research, providing a deeper understanding of the tools and techniques employed to address the challenges and opportunities in the intersection of cybersecurity, communication networks, and healthcare technology, especially in the context of remote patient monitoring.

1.8.2 Chapter 3: Research Methodology and Research Design

This chapter provides a detailed research methodology and research design of this work. It showcases the various phases of research work and how this research will be achieved based on the designed workflow. It describes the different research stages involved in establishing a semantic framework to achieve the desired outcomes. The initial phase is a literature review followed by the conceptual framework. Based on the conceptual framework, a prototype is developed, and validation is performed by a case study.

1.8.3 Chapter 4: Developing a Novel Ontology for Cybersecurity in Internet of Medical Things-Enabled Remote Patient Monitoring

In this chapter, the MIoT ontology applies the Knowledge Engineering Methodology as described in Ontology Development 101, alongside a structured life cycle, to foster semantic interoperability among medical devices and safeguard IoMT assets against vulnerabilities and cyberattacks. Defining crucial concepts and relationships simplifies the comprehension and analysis of the complex information network within the IoMT. The MIoT ontology captures vital terms and organizes security-related entities to facilitate future extensions by emphasizing potential advancements in security automation within healthcare applications, such as remote patient monitoring systems. Based on knowledge the conceptual model is proposed and validated against the case study.

1.8.4 Chapter 5: Knowledge Organization System for Partial Automation to Improve the Security Posture of IoMT Networks

Utilizing ontology development principles, a prototype was constructed involving concepts relevant to IoMT and cybersecurity. Object and data properties were established using standard formalisms such as RDF and OWL. Automated reasoning was then applied to validate a hypothetical scenario.

1.8.5 Chapter 6: Novel Knowledge Graph-Based Modeling for Vulnerability Detection in the Internet of Medical Things

This chapter presents the development of a semantic framework for vulnerability detection in Internet of Medical Things (IoMT) environments, along with a discussion of initial experimental results. The framework utilizes semantic modeling to improve data annotation and knowledge base creation, thereby supporting the detection of vulnerabilities in medical IoT networks. Additionally, it generates a knowledge graph that stores Cyberthreat Intelligence (CTI) for these networks, providing a query mechanism to extract insights from the knowledge graph.

1.8.6 Chapter 7: Implementation, Testing and Validation

This chapter presents the implementation of the complete semantic framework. It includes a semantic model, ruleset generation, and reasoning over the aggregated knowledge. The knowledge graph is developed, vulnerability data is integrated via API, and knowledge graph representation and querying are performed through the SPARQL endpoint.

To evaluate the MIoT ontology, ontology engineering practices are used. Subsequently, after evaluating the ontology, automated reasoning is performed and results are compared with the Generative AI Model. This study utilizes this additional validation and performance analysis with the Generative AI model to assess the effectiveness of rule-based reasoning compared to the Generative AI model.

Finally, the proposed semantic framework is validated against the existing framework in the domain of IoMT where the research focuses on vulnerability detection.

1.8.7 Chapter 8: Results and Findings

This chapter discuss a thorough presentation of the conclusive outcomes and insightful discoveries derived from the research efforts and comprehensive experimentation conducted throughout the study. The limitations of the research work are also discussed here.

1.8.8 Chapter 9: Conclusion and Future Work

This chapter concludes the dissertation by providing an overview of the challenges and the solutions proposed in this thesis. This chapter also highlights possible avenues for future research.

1.9 Summary of the Chapter

This chapter provides a comprehensive overview of the Internet of Medical Things (IoMT), emphasizing its critical importance and widespread application in the healthcare domain, including Remote Patient Monitoring. It explores the research problem and outlines the key research issues, leading to the formulation of targeted research questions aimed at addressing these specific challenges.

Additionally, this chapter discusses the significance of IoMT in relation to vulnerabilities and cyber-attacks, focusing on remote patient monitoring systems and their prevalent cyber threats. The chapter concludes by highlighting the importance and potential impact of this research work in advancing the security and effectiveness of IoMT in the healthcare sector. It also outlines the contributions and structure of the thesis.

Chapter 2

Literature Review and Background

This chapter provides information about the background of this research from both theoretical and technological perspectives. It presents a panoramic view of existing works, methods, and technologies used in the domain of IoMT and cybersecurity. In this regard, Section 2.3 contents are published as a book chapter, available at: `http://doi.org/10.1007/978-3-031-24946-4_5` and adjusted according to thesis requirements.

Additionally, this chapter includes a scoping review section 2.5, which provides an overview of IoMT and cybersecurity as an interdisciplinary research area. This section presents details of the literature review, including the selection, annotation, and synthesis of studies, to offer peer-reviewed quality information in this thesis. The scoping review helps identify the research gaps and establishes the novelty of this work. The scoping review protocol is published in a Journal [48], and available at: `https://rsdjournal.org/index.php/rsd/article/view/46080`

2.1 Internet of Medical Things (IoMT)

Nowadays, IoMT plays a key role in managing healthcare data. IoMT includes various medical devices, applications, and sensors such as wearables, ambient sensors, mobile apps, and portable devices [49], [50], [34]. IoMT improves accuracy and accessibility in healthcare, facilitating telehealth services for distant patient-doctor consultations with the help of these devices. Medical IoT devices are well suited for patient monitoring and diagnosis, particularly because they collect, transfer, analyze and interact with, (near-)real-time data [51] even in remote areas. IoMT's integration into healthcare represents a significant advancement, connecting various medical devices and applications through the internet for improved health management.

The Medical IoT (IoMT) network is composed of various devices designed to provide real-time solutions for patient diagnosis and monitoring. These devices differ in design, architecture, sensor type, workflow, implementation, and application. Common devices used to collect patient information include computing devices, mobile phones, wearables, surveillance cameras, motion and body sensors, implantable surgical devices, actuators, and smart glasses. These devices efficiently transmit vital signs data from patients to hospital staff (e.g., doctors, and nurses) to facilitate remote health monitoring. They can perform operations such as detecting temperature, glucose levels, heart rate, blood pressure,

and pulse rate.

The core of an IoMT-based healthcare system is its architecture, which is essential for understanding IoMT applications and technology. Researchers [52], [53], [54],[55],[56] have adopted and proposed various standardized IoMT architectures and frameworks. Most IoMT systems are structured into four layers: the perception (sensor) layer, the network (communication) layer, the platform layer, and the application layer. Figure 2.1 illustrates a general IoMT architecture containing four layers: Perception Layer, Network Layer, Platform Layer and Application Layer.

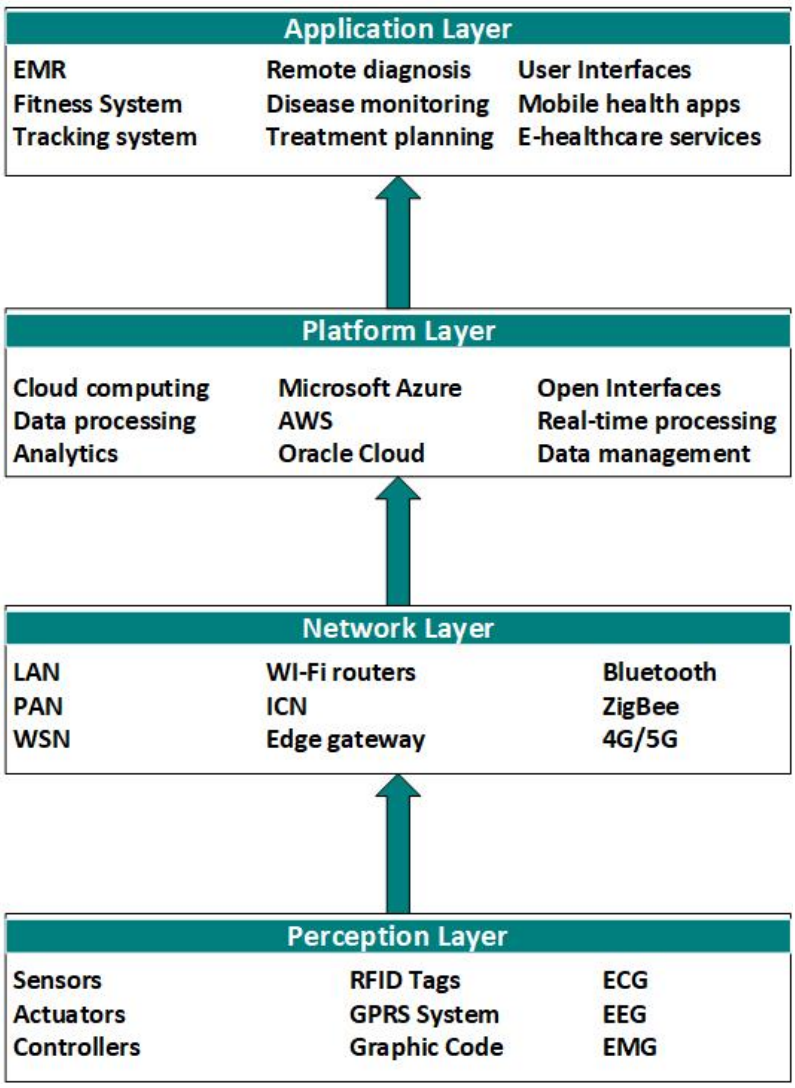

Figure 2.1: General architecture for the Internet of Medical Things (IoMT).

a. Perception Layer

This foundational layer is also called the sensor layer or device layer, critical for collecting data from the source, ensuring a comprehensive view of health-related metrics. This layer includes various hardware components such as sensors, controllers, and actuators. Current devices include RFID readers/tags, GPRS systems, facial recognition cameras, fitness smartwatches, health-monitoring sensors, insulin pumps, and infrared temperature sensors. The main function of this layer is to perceive and interpret collected data using medical perception and signal acquisition equipment. Technologies like Bluetooth, Wi-Fi, Zigbee, and 4G/5G networks are

used for efficient short-range data transmission [34]. These devices empower individuals to track their physical wellness and monitor their health digitally. Examples include smart watches, smart shoes, and various sensors like ECG, EEG, airflow, blood pressure, motion, and activity sensors. These IoMT-enabled sensors have comprehensive identification, sensing, and communication capabilities, allowing for the capture of vital signs from homes, hospitals, or any remote location.

b. Network Layer

Building on the perception layer, the network layer ensures real-time and accurate data transmission. It uses various mediums, including the Internet, mobile communication networks, local area networks, access networks, and wireless sensor networks. This layer integrates different networks, standardizes information description formats, and manages data warehouses. It also provides services related to platforms and open interfaces to facilitate integrations [34].

Recent innovations in IoT communications have introduced efficient, low-power protocols such as Wireless Sensor Networks (WSN), Bluetooth, ZigBee, WiFi, NB-IoT, LTE, 4G, and 5G, designed for wireless networks like Body Area Networks (BAN) and Personal Area Networks (PAN). Key to connecting multiple devices are aggregation points, with WiFi routers being crucial gateways. The emergence of Information-Centric Networking (ICN) brings a data-centric approach to IoT communication, enhancing scalability, routing, mobility support, caching strategies, and security [34],[55].The IoMT edge network includes edge gateways like smartphones, tablets, or laptops, which receive and forward vital sign data via shorter-range communication protocols such as Bluetooth, 6LoWPAN, or Wi-Fi to healthcare provider's cloud platform services.

c. Platform Layer

The IoT platform layer offers essential services such as cloud computing and middleware technology. Cloud platforms like Microsoft Azure, Oracle Cloud, Amazon Web Services, Google Cloud, IBM Cloud, and Alibaba Cloud are pivotal in delivering messaging, storage, data processing, and analytics services for IoMT applications. This layer is responsible for data processing and storage, providing authorized healthcare professionals with access to patient data for diagnosis and treatment, thereby enhancing healthcare delivery efficiency.

d. Application Layer

The topmost layer leverages data from the platform layer to manage medical records through various applications. It integrates healthcare equipment and resources to maintain comprehensive patient information, including data management for inpatient and outpatient services, medical treatment processes, tracking systems, fitness and health systems, remote diagnostic systems, telemedicine, and electronic medical records. This layer focuses on analyzing patient data, disease characteristics, medication details, diagnostics, and treatment options to facilitate informed decision-making in medical contexts.

Researchers [57],[58], [59] explore this field under the umbrella of wireless sensor networks (WSN), which include subsets such as medical smartphone networks (MSN) and wireless body area networks

(WBAN). These networks comprise wearable devices worn by individuals and interconnected with each other. For example, WBANs (Wireless body area networks), i.e., sensors and actuators are suitable for medical and e-healthcare applications in terms of remote patient monitoring. A Wireless Body Area Network (WBAN) comprises sensors that can be worn or implanted in a living body to gather diverse biosignals, including electrocardiogram (ECG), electromyogram (EMG), electrooculogram (EOG), electroencephalogram (EEG), and magnet encephalogram (MEG). These signals are transmitted to an end server through a gateway sensor node for analysis by a healthcare specialist [46]. Technology such as wireless sensor networks (WSNs) allows these WBANs to transfer data through the network [36], [60].

However, IoMT devices, similar to general IoT systems, are vulnerable to hacker attacks. The risks are heightened in IoMT due to their direct connection to the human body and the sensitive nature of the data they handle. Software in IoMT devices is critical and prone to both accidental and intentional breaches. Hardware and software vulnerabilities can lead to data theft or manipulation, and disruption of the medical device's function. The future connectivity of IoMT devices, which is likely to involve advanced technologies like 6G, Wi-Fi 6, Bluetooth 5.2, and Satellite Internet, also presents potential targets for cybercriminals [61].

2.1.1 Remote Patient Monitoring Systems

A lack of effective health monitoring is a significant challenge faced by patients worldwide. IoT, cloud computing, and WBAN devices offer a sustainable solution by enabling remote monitoring for medical professionals. Remote Patient Monitoring (RPM) is one of the applications in the Internet of Medical Things, where a continuous stream of real-time information about patients can be transferred through medical devices connected with IoT sensors [62], [63]. RPM is a healthcare delivery model that uses technology to collect and transmit patient data from a remote location to healthcare providers for analysis and treatment [15]. This allows healthcare providers to monitor patients' health status and manage their care remotely, without the need for in-person visits. Examples of RPM technology include wearable devices (such as fitness trackers), smartphones, and home-based monitoring equipment (such as blood pressure cuffs) [50],[64]. These technologies can detect the patient's condition and behaviours by monitoring their blood pressure, heart rate, etc. In case of any abnormal reading (which might be caused by not only a system error but also hacking), a doctor or caregiver will be alerted for assessment [39].

Remote monitoring facilitates timely and efficient preventive measures, significantly enhancing the quality of care and improving patient outcomes. It offers a significant benefit in managing various diseases by reducing the need for frequent clinical visits. These devices closely monitor a patient's health status and relay this information to designated contacts, including healthcare professionals. By analyzing the data with sophisticated algorithms, RPM systems can promptly identify any health deterioration or abnormalities, facilitating timely intervention. This technology brings healthcare services directly to patients, enhancing care quality and convenience. RPM devices are versatile, serving individuals across all age groups. The goal of RPM is to improve patient outcomes, increase access to care, and reduce healthcare costs [65]. However, a critical aspect of using these technologies

is ensuring the privacy and security of sensitive health data, which remains a significant challenge in their deployment and use. It is very difficult to maintain data security, scalability, heterogeneity, interoperability, and integration throughout a network due to the exposure of data, and various types of devices with different functionality and specifications [39], [66].

Cyberattacks in Remote Patient Monitoring Systems

Remote patient monitoring (RPM) systems rely on a network infrastructure to gather and transmit data from patients to healthcare providers through a network. As these systems become more prevalent, they may also become targets for cyberattacks. Here are a few examples of cyberattacks on RPM systems [67], [68].

1. Man-in-the-middle attacks: In a man-in-the-middle (MITM) attack, an attacker intercepts and alters the communication between the patient's device and the healthcare provider's system. This can allow the attacker to steal sensitive patient information or alter the data being transmitted, leading to incorrect treatment decisions.

2. Denial of service (DoS) attacks: A DoS attack is designed to disrupt network services by overwhelming a system with traffic. In the context of RPM systems, a DoS attack could disrupt the transmission of patient data and prevent healthcare providers from receiving important information.

3. Tampering: Tampering with or physically damaging sensors or devices, can lead to inaccurate data being collected or transmitted.

4. Device spoofing: An attacker could create a fake RPM device and connect it to the network, allowing them to steal sensitive information or disrupt the system.

5. Network mapping: An attacker could use network mapping techniques to discover the layout and structure of the network infrastructure used by the RPM system. This could allow the attacker to identify vulnerabilities and launch more targeted attacks.

6. Malware injection: An attacker could infect the RPM system with malware, which can steal sensitive information, disrupt the system, or provide the attacker with remote access to the network.

7. Phishing: An attacker could launch a phishing campaign to trick employees or patients of the RPM system into providing their credentials. This would allow the attacker to gain access to the network and steal sensitive information.

8. Eavesdropping attacks: An attacker intercepts the communication and listens in on the transmission of data.

9. SQL injection attacks: An attacker injects malicious code into a database, allowing them to extract sensitive information or manipulate data.

10. Cross-site scripting (XSS) attacks: An attacker injects malicious code into a website, allowing them to steal user information or control the website.

Apart from this, modern security attacks on smart healthcare systems have evolved beyond typical attacks such as DDoS, MITM, and ransomware. Attackers have devised new methods to exploit system vulnerabilities. Recent attacks include software supply chain attacks, where attackers exploit the supplier network of healthcare institutions. Additionally, Internet of Things (IoT) attacks have become prevalent, as a wide range of endpoint devices are now remotely connected to the Internet. Malware deployed in these attacks interprets system changes and manipulates received signals to execute destructive activities [69].

2.2 Medical Device Categorization

A medical device is a broad term that includes a wide range of instruments, apparatuses, machines, software, implants, or other similar items used for medical purposes. These devices are designed and manufactured to diagnose, treat, monitor, or mitigate medical conditions, diseases, or disabilities in patients. Medical devices can be categorized based on their usage, placement, and functionality. Such medical devices have different configurations and features according to their usage and functionality. The most prominent vendors along with their product settings are shown in Appendix A. This study focused on different existing works and gave an overview of those medical devices that are usually used in IoMT, particularly in remote patient monitoring settings, not the detail because it is out of scope for this work. These medical devices are categorized based on their usage, placement, and functionality.

2.2.1 Common Medical Devices based on Usage and Placement

The medical devices that fall into this category include implantable, ambient, wearable, portable, and mHealth devices. This categorization is based on whether the medical device is used in the environment, attached to the body, or placed in a hospital [35], [70], [71], [72], [73]. Each category serves different needs and offers various levels of convenience and monitoring capabilities.

a. **Implantable Devices**

   Implantable devices are a significant aspect of modern medical technology, offering a range of therapeutic and diagnostic functions. They are surgically placed inside the human body and are designed to perform various health-related tasks [70], [73]. Pacemakers, defibrillators, drug delivery systems, neurostimulators, and infusion pumps are some examples of implantable devices.

b. **Ambient Devices**

   Ambient devices refer to a category of technology that seamlessly integrates into a user's environment to provide information or services without requiring direct interaction. These devices are designed to blend into the background of everyday life, enhancing the user experience through

unobtrusive and intuitive interfaces. By continuously monitoring the patient's environment, these devices track activity patterns, sleep quality, bathroom visits, and more, promptly alerting caregivers to any deviations from normal behavior. These sensors are expected to revolutionize the healthcare landscape, making patient rooms more intelligent and secure, particularly for individuals managing chronic conditions [71], [74]. Ambient sensors include motion sensors for dementia and Parkinson's disease, as well as room temperature and pressure sensors.

c. **Wearable Devices**

Wearable sensors are increasingly important in healthcare for real-time tracking of vital diagnostic signals, enabling cost-effective and widespread monitoring by connecting various devices. These sensors have evolved to monitor a wide range of data, including physiological signals such as ECG[1], EM[2], and EEG[3], chemical indicators like blood sugar levels, and optical data such as oximetry [71], [75], [76]. They are also used for tracking motion, physical activity, location, and managing therapies and treatments like drug delivery and chronic pain relief [77].

One key application of these wearable technologies on the Internet of Medical Things (IoMT) is to alert healthcare professionals in medical emergencies through on-body and peripheral sensors and help to improve the healthcare industry by reducing the load on medical staff [34]. These technologies are particularly beneficial for elderly patients with conditions like Parkinson's, Alzheimer's, and Dementia, as well as for cognitively challenged individuals, aiding them in daily living activities. These technologies are also valuable for monitoring the health and movement of healthy individuals, contributing to the development of smart clothing and other wearable devices [49].

d. **Mobile Health (mHealth) Applications**

These mobile health apps, designed to run on smartphones or tablets, serve a multifaceted purpose in the realm of healthcare. They function as tools for monitoring various health metrics, such as heart rate, blood pressure, and physical activity [78]. Additionally, they provide functionalities such as reminders for medication intake, helping patients adhere to their prescribed treatment plans effectively. Furthermore, these apps often facilitate seamless communication between patients and their healthcare providers, enabling users to share health data, ask questions, schedule appointments, or receive virtual consultations.

For instance, Apple and Google have developed dedicated platforms such as Apple's ResearchKit and Google Fit to create research applications for gathering fitness and health statistics. These applications enable seamless interaction with various consumer devices and embedded sensors, facilitating the integration of data. This accessibility allows doctors to have direct access to comprehensive health data, providing both healthcare providers and users with real-time insights into the user's health status. Moreover, these apps and smart devices play a significant role in

[1]Electrocardiogram
[2]Electromyogram
[3]Electroencephalogram

enhancing wellness planning and promoting healthy lifestyles. Consequently, users or patients are empowered to take an active role in managing their health [79].

2.2.2 Common Medical Devices based on functionality

Medical devices used in remote patient monitoring can be categorized as actuators, medical sensors, or a combination of both based on their functionality. The categorization of these devices is based on their primary function - whether they are primarily for sensing (monitoring) health metrics or acting upon the collected data to adjust or control a function or treatment [59], [80].

a. **Actuators**

Actuators are devices that actively control or adjust a physical process based on received input. The actuators function according to input from either the occupants or the central computing system. This central system gathers environmental, physiological, and activity data via the PAN /WSN, processes it, and can provide feedback to the user or trigger the actuators to manage devices like a humidifier, oxygen generator, oven, and air conditioner [54]. In medical settings, actuators might not be as commonly used in remote patient monitoring as sensors. However, an example could include certain types of drug delivery systems, such as Insulin pumps, which actively administer medication based on monitoring data [59], [73].

b. **Medical Sensors**

In smart technologies, medical sensors such as wearables are energy efficient and active to facilitate long-term monitoring. mainly monitor and gather health data using WBAN technology to achieve automated, continuous, and real-time measurements of physiological signals such as ECG, and EEG [59]. Examples of those medical sensors include:

- Blood Glucose Meters: Measure blood sugar levels.
- Pulse Oximeters: Measure oxygen saturation in the blood.
- Blood Pressure Monitors: Measure blood pressure.
- Heart Monitors: Monitor cardiac activity.
- Specialized Monitors for conditions like dementia or Parkinson's: Track movement or other specific health indicators.

c. **Actuator and Medical Sensor**

Actuators and medical sensors are devices that both collect data and actively respond to it. These medical sensors and actuators have been suggested for healthcare, capable of monitoring both vital signs and patient activities. These systems integrate sensors, software, and wireless technology to gather, process, analyze, and transmit physiological and activity data to a remote healthcare center. Intelligent homes could integrate wearable systems connected via WBAN, along with environmental sensors, actuators, and cameras, all interconnected through a WSN [11], [35], [59], [81]. For example:

- Implantable Cardioverter Defibrillators (ICDs): These not only monitor heart rhythms but can also deliver a shock to the heart if a life-threatening irregular rhythm is detected.
- Advanced Pacemakers: Monitor heart rhythms and provide electrical stimulation when necessary.

2.3 Cyber-Resilience for IoMT is an Interdisciplinary Research

Detecting vulnerabilities and cyberattacks requires a thorough understanding of the underlying systems and frameworks. The Internet of Medical Things (IoMT) and Remote Patient Monitoring (RPM) are rapidly growing fields that encompass a vast array of existing work, protocols, and standards. IoMT plays a crucial role in healthcare, assisting professionals with various medical procedures and patient care to ensure the well-being of patients [82].

2.3.1 Cyberattacks in Real-time Healthcare Applications

The Medical IoT network is very large and complex and contains various types of sensors, interconnected devices, and end-user applications. However, this presents challenges as data is transmitted through communication technologies. Attackers can attempt to manipulate, steal, interrupt or transmit data. These actions are possible due to vulnerabilities in IoT medical devices, and as a result, cyberattacks occur and reoccur. Alromaihi et al., [31] have categorized these attacks into two types; internal attacks and external attacks. Password sniffing, data tampering and Trojan horses are some examples of internal attacks; while Denial of service (DoS), remote brute-force attacks, man-in-the-middle (MIM) attacks, false data injection, eavesdropping and spoofing are examples of external attacks. The literature shows that the most common types of attacks are Denial of service (DoS), Eavesdropping [28], [83], Phishing [67], [68], SQL Injection [84], and Malware such as backdoors, viruses, Trojans, spyware and worms [83].

In Australia, according to ACSC (Australian Cyber Security Centre), hospitals and aged care facilities are the lucrative targets for cybercriminals. Due to the COVID-19 pandemic, there has been a significant increase in malicious cyber activities in healthcare using Maze ransomware [85]. In this regard, the ACSC provides some guidelines to protect from ransomware such as backup files, using patching software, installing antivirus and checking updates [86]. However, it is important to note here that remote patient monitoring solutions within IoMT primarily rely on wired or wireless communication networks. These IoMT devices typically transmit their data over the Internet using Internet Protocol (IP) networks, although some devices establish local connections using technologies like Bluetooth and RFID [68]. A central challenge in IoMT is the seamless transfer of data between devices. This includes the transfer of patient data from various medical devices, such as glucometers, to devices like PDAs, laptops or computers, utilizing a range of connectivity options such as Bluetooth, Wi-Fi, cloud or fog computing. This data transfer is crucial for enabling real-time analysis and healthcare predictions.

2.3.1.1 Cyberattacks on Medical Devices

In a smart home environment, medical devices are connected through the network to transfer data and information from patients to the server/hospital. Medical devices are repeatedly facing challenges in terms of cyberattacks in healthcare. Prime examples are medical imaging devices (MIDs), including MRI machines and CT devices. In 2017, the WannaCry ransomware attack was spread over 150 countries and infected 200,000 medical devices, which included 10,000 hospital devices from the UK's National Health Service (NHS) and MIDs that became non-operational after encryption. Furthermore, this attack diverted multiple ambulance routes and turned away patients from hospitals [87].

In April 2018, security threats about defibrillators of Abbott Implantable Cardioverter Defibrillators (ICDs) were recorded. These affected medical devices were made up of in-built programmable computer systems, vulnerable to cyberattacks because they were connected to hospitals via the Internet. The unauthorized user could easily take control of such devices by using equipment that was available commercially. Where the unauthorized user performed various acts through a defibrillator, such circumstances could have resulted in patient deaths [73].

In March 2022, Researchers from CyberMDX, a healthcare security firm, found seven easily exploited vulnerabilities (called Access:7). These were found in the PTC Axeda remote access tool. Such vulnerabilities could potentially allow the extraction of data from medical equipment, the tampering of lab results, or the making of critical devices unavailable. The researchers estimated that the Access:7 vulnerabilities could compromise thousands of devices out in the field [88].

2.3.1.2 Cyberattacks in Hospitals

In the healthcare industry, where medical devices are frequently targeted by attackers, hospitals and their Internet-connected equipment such as computers also face significant cybersecurity threats. Over time, Electronic Healthcare (E-Healthcare) applications have seen increasing development and utilization as efficient and effective methods for requesting medical services. They do this by conducting clinical trials and sharing sensitive patient information among interconnected stakeholders [89]. In February 2016, a $17,000 (40 Bitcoin equivalent at the time) ransom was reported to be paid by the Hollywood Presbyterian Medical Center [39], [90]. The hackers took over the control of the computer systems of the hospital via malware, and as a result, the institution's staff could not communicate through those devices. The hackers gave back access only after the ransom was paid [91], [87].

A month later, the computer network of MedStar, a nonprofit hospital in the USA, was hacked. The hackers asked for a 45 Bitcoin ransom to return all data safely to the 10 hospitals and around 250 outpatient centers. Due to this attack, they shut down many of the computer systems when they received the message from the attacker. While malware attacks like this may be less impactful for other businesses, in healthcare, they are related to patient healthcare at the highest level. Since patients' e-health records are disturbed due to these attacks, they render patients unable to communicate with remote hospitals and prevent or restrict access to medical services provided by them [92].

Due to infrequently updated software and standards, in April 2017, many computers and medical devices in hospitals in the UK were vulnerable and affected by the EternalBlue exploit tool leaked by a hacker group known as the Shadow Brokers, which emerged alongside several other exploits.

EternalBlue (CVE-2017-0144) is an exploit of the Windows Server Message Block (SMB) protocol which affected various Windows versions, such as Windows Server 2008, Windows Server 2012, Windows 10, Windows Server 2016 and Windows Vista. In the previous month to the widespread realization of the EternalBlue exploit, Microsoft issued a critical security patch to fix the vulnerability. Despite the notification from Microsoft, some users did not access the update, and many computer systems remained vulnerable [93].

The 2020 cyberattack targeting the University of Vermont Health Network left affected individuals in a precarious situation for over 40 days. With more than 5000 computers rendered inoperable, nearly 300 employees faced joblessness for an extended period. Experts calculated the financial toll of the cyberattack at 1.5 million dollars per day, encompassing both revenue losses and additional expenses. Additionally, Universal Health Services, based in King of Prussia (Pennsylvania), encountered a substantial malware attack in 2020 that lasted for eight days [94].

In 2018, Hancock Health in Greenfield, Indiana, acknowledged paying a ransom of $55,000 in Bitcoin following a ransomware attack in January. The incident began on the evening of January 11, when hospital staff noticed a significant slowdown in their computer systems. Shortly thereafter, the screens displayed a ransom note that indicated a security breach. This resulted in an attack that targeted over 1,400 files. The cyberattack impacted various systems, including the hospital's email, electronic health records, and internal operating systems. In response to the cyberattack, Hancock Health reverted to manual record-keeping with pen and paper, a procedure they routinely practice, which helped minimize administrative disruptions [95].

In the field of research, BEdgeHealth, a decentralized health architecture is proposed by Nguyen et al., [96], integrating MEC[4] and blockchain for data offloading as well as sharing these elements in distributed hospital networks. The proposed data offloading scheme allows mobile devices to efficiently offload health data to nearby MEC servers with privacy awareness. Additionally, a data-sharing scheme facilitates exchanges among healthcare users using blockchain and interplanetary file systems. The integration of a smart contract-based authentication mechanism with MEC enables decentralized user access verification at the network edge, eliminating the need for a central authority. Real-world experimental results validate the effectiveness of the BEdgeHealth architecture, showcasing improved QoS with data privacy and security guarantees compared to existing schemes.

Another researcher Weber et al, [58] investigates the current state of research in detecting attacks on medical devices in hospitals and clinics, focusing on the challenges of hospital networks, attached medical devices, and the variety of protocols used by these devices. Here the authors acknowledge challenges such as device heterogeneity and lack of standard datasets, making centralized management and effective security testing difficult. The paper concludes by suggesting future work, including creating MCPS[5]-specific datasets, standardizing security protocols, and developing tailored intrusion prevention strategies to enhance hospital IT security and patient safety. In critical terms, this work fails to identify several of the important issues related to vulnerabilities or threats in medical devices connected to the network remotely.

[4]Mobile Edge Computing
[5]Medical Cyber-Physical Systems

2.3.1.3 Cyberattacks in Aged Care Facilities

The Australian Cyber Security Centre (ACSC) has identified aged care facilities and hospitals as primary targets for cybercriminals, with a noticeable increase in attacks during the COVID-19 pandemic. Maze ransomware exemplifies vulnerabilities in this sector, as malicious actors use it to encrypt files and lock critical information, enabling them to demand ransomware. To counter these threats, the ACSC provides guidelines that include backing up files, patching software, installing antivirus programs, and keeping systems updated [86]. Despite these efforts, persistent attacks indicate that aged care facilities continue to be prime targets for malicious actors.

In August 2020, Regis Healthcare, a publicly listed aged care provider, announced that it was the victim of a cyberattack. A foreign actor had copied some data from Regis Hospital's IT system and released personal information. The healthcare provider used their backups to maintain business continuity, so the attack had a reduced impact on resident care and service delivery and did not affect day-by-day operations. This incident led to the Australian Federal Government and aged care's technology peak body issuing a warning to providers to take precautions against such attacks. The Australian Cyber Security Centre noted a significant increase in ransomware attacks targeting the aged care sector. Recommendations included not paying ransom demands, backing up critical information, regularly updating systems and software, and using up-to-date antivirus software. The report highlights the vulnerability of Australia's aged care providers to cyberattacks [97].

2.3.2 The Role of Legislation and Standards for Cyber-Resilience in Medical Smart Homes

The medical smart home sector has experienced a shift towards an increased heterogeneity of OT[6] devices in healthcare, including the diversity of connectivity types and the broad variety of terminology. The heterogeneity of devices and missing regulations have led to a situation where there is a very small effort toward the central management of devices from assorted manufacturers. Furthermore, the different requirements based on the application of different devices have led to augmented requirements for connectivity [91]. For example, computed tomography scanners are regularly connected via a wired connection and wearable medical devices require a wireless connection [58].

Smart homes contain a wide variety of electronic devices, including computers, smartphones, actuators, and sensors, as well as software used in communication networking and medical applications [50], [59], [98]. All of these devices are vulnerable to cyberattacks for several reasons. First, devices used for collecting medical data typically rely on Bluetooth or cloud networks, neither of which is fully secure. Second, many people using electronic medical devices are unfamiliar with technology, often resulting in non-compliance with protocols or standards. Furthermore, patient data transferred through wireless communication channels is inherently exposed to cyber threats. As a result, data replacement, data updating, and data theft are among the main risks in these systems.

The growing number of cyberattacks and new waves of ransomware have raised concerns among government agencies and regulators. In response, regulatory bodies have taken action to establish

[6]Operational Technology

policies and standards that protect critical infrastructure and services like healthcare. The Australian Government's TGA[7] Health Safety Regulation provides standards recognized as best practices for manufacturers to meet regulatory requirements for the cybersecurity of medical devices. Similarly, the U.S. Food and Drug Administration (FDA) has developed guidelines for medical device manufacturers. These pre-market and post-market guidelines offer recommendations for managing cybersecurity risks throughout a medical device's life cycle [99].

To ensure secure communication between patients, medical devices, and aged care facilities, manufacturers must follow the standards and protocols defined by regulations and laws. The interaction between medical devices, sensors, servers, gateways, and applications can achieve a high level of security if standard protocols are followed [58]. Compliance with health industry standards and protocols set by the government and relevant authorities is essential to ensure connectivity reliability.

For instance, "electronic protected health information" (e-PHI) recognizes all health information created, maintained, updated, or converted into electronic form as a covered entity. This is part of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) [100]. Integrating the standards proposed through HIPAA is crucial to protecting information from threats and attacks [37], [31], [101], [102]. Security requirements for medical devices can be categorized as follows:

a. *Confidentiality:* To ensure the protection of information from unauthorized users and devices. In this situation, attackers cannot gain unauthorized access to sensitive information.

b. *Integrity:* To ensure the data is accurate and real, the received data does not include any false insertion, modification, or deletion. This is needed to prevent a situation where the attacker can interfere with some sensitive information without authorization. One such example is code injection, where the attacker can insert malicious data/code to compromise the data integrity of the sensor node. Since most systems guarantee privacy, these systems are vulnerable to tampering. Integrity refers to the accuracy and completeness of the system during communication.

c. *Availability:* In this mechanism, only those users who have access to the IoT systems/websites when needed should be given access. This prevents those who compromise the confidentiality and integrity of the IoT system. Where someone is not able to compromise these properties, other types of attacks can be launched by a malicious actor to make the system unavailable to users, such as a denial-of-service attack.

d. *Privacy:* Applications in healthcare now use multiple forms of communication media to transfer data, which can eventually lead to privacy issues, such as the tracking of a device's location. This can lead to instances that can damage a patient's circumstances by implying the unwanted use of their private information. IoT health applications must impose policies to ensure the privacy of patients, especially where patient data access is requested according to those policies.

e. *Identification:* This ensures the identity of all entities, i.e., patients, health workers, doctors, and caregivers using the system, before initiating any communication and permitting interaction with the resources of the system.

[7]Therapeutic Goods Administration

f. *Authentication:* The authentication procedure validates the identities of communicating parties before starting the communication of messages. Various techniques are used to safeguard data from non-authentic users or resources. Steganography is one example, where existing data is transformed into multimedia data that is difficult to process by sensor nodes due to limited resources.

g. *Accountability:* The process requires each entity, i.e., patients or doctors, to be responsible for their actions and to take note and observance of any abnormal activity in the IoT system.

h. *Auditing:* This refers to the ability of a system to track and monitor all activities and record events in real-time. This includes the login details, the health information of the patient, and the doctor's investigation.

i. *Authorization:* This forms a security mechanism that determines whether the accessing privileges of either a user or a device are authentic and therefore appropriate to use the system's resources. This process is called authorization. This access is granted by authorities such as a system administrator, who handles all the users and devices of the system.

j. *Data Freshness:* In this mechanism, recent and fresh information is stored in systems, preventing old data from being replayed. For example, the current situation of the patient should reflect their pulse, heart rate, and blood pressure, which can be uploaded to the IoT system.

k. *Non-repudiation:* In this mechanism, a malicious actor should be prevented from denying the validity of incoming messages. It assures the origin and integrity of messages, sometimes called ISS (information security service). The authenticity of a digital signature during an online transaction is one example. It can be further divided into two types: non-repudiation of origin, which guarantees the message is sent by an authentic sender, and non-repudiation of destination, which assures the message is received by an authentic receiver.

These security requirements are crucial to protecting sensitive data, preventing breaches, complying with regulations, maintaining reputation, ensuring business continuity, and saving costs. Robust security measures enable medical IoT devices to safeguard against vulnerabilities and cyberattacks and reduce the risk of security breaches.

2.3.3 Knowledge Organization Systems for Cyber-Resilience in Medical Smart Home Environments

In smart home applications like remote patient monitoring, the Internet of Things (IoT) plays a vital role. IoT integrates diverse technologies such as RFID[8], WSNs[9], big data, cloud services, and various application-based technologies capable of capturing and recognizing data from smart home applications. The need arises to standardize and structure data from diverse sources for efficient aggregation and fusion.

[8]Radio Frequency Identification
[9]Wireless Sensor Networks

Semantic Web technologies illustrate effective methods for representing and organizing data from different sources, including medical IoT sensors [66]. Semantic search engines and browsers facilitate semantic traversal, with agents functioning as programs for transferring meaningful data [95]. These software agents automate system management by acquiring, querying, and reusing existing knowledge to accurately capture the semantics associated with medical IoT devices and their properties.

Over the years, numerous knowledge organization systems recommended by W3C[10] and a semantic web standard have emerged to facilitate data exchange, fusion, and automation for cyberthreat intelligence.

"The term 'knowledge organization systems'[11] is intended to encompass all types of schemes for organizing information and promoting knowledge management" [5], [6]. They include classification schemas, taxonomies, semantic networks, and ontologies, each varying in abstraction, scope, and intended purpose [7]. Figure 2.2 illustrates the various features of Knowledge Organization Systems (KOS).

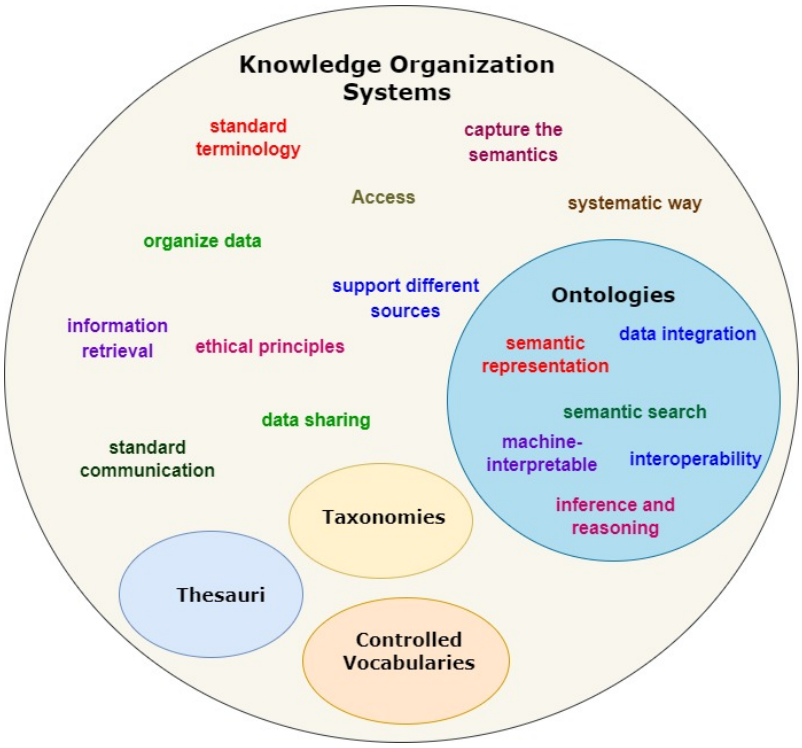

Figure 2.2: Knowledge Organization Systems features adapted from [5], [6], [7] .

2.3.3.1 Semantic models for IoMT

The semantic web [103], also known as Web 3.0, is an extension of World Wide Web (W3C) standards[12]] Semantic web - W3C, [https://www.w3.org/standards/semanticweb/]. The semantic web is a web of data that extends the current web to provide a common framework for organizing, representing,

[10]https://en.wikipedia.org/wiki/World_Wide_Web_Consortium

[11]The term 'knowledge organization systems,' as used in this report, was coined by the Networked Knowledge Organization Systems Working Group at its initial meeting at the ACM Digital Libraries '98 Conference in Pittsburgh, Pennsylvania.

[12]Semantic Web at W3C: https://www.w3.org/standards/semanticweb/

sharing, and reusing data across diverse applications and systems [104], [105]. Semantic Web technologies are among the examples to represent and organize the data coming from different sources. Retrieving heterogeneous information from cross-domain applications is critical, and semantic web technologies are instrumental in linking web data that facilitates the representation of relationships within web data [104].

Semantic models play a crucial role in making web content more machine-understandable and encoding information on the web by using standards like RDF (Resource Description Framework) and OWL (Web Ontology Language). A semantic model is a high-level, abstract representation of data that focuses on capturing and conveying the meaning or semantics of information rather than just its structure or syntax, allowing the interpretation of meaning from instances. In data integration and data exchange scenarios, semantic models help ensure that data from different sources can be understood and integrated effectively. By encoding the meaning and relationships between data elements, semantic models enable interoperability between systems [39].

Ontologies are one example of a semantic model, a fundamental component of the Semantic Web, where they enable machines to understand and process web content, leading to more intelligent web services and applications. By encouraging a common understanding of concepts and relationships, ontologies facilitate interoperability between diverse systems and databases. In medical settings, data acquired from various sensors and medical devices necessitates semantic approaches to address interoperability challenges arising from heterogeneous sensor data in IoT devices. This data should be represented using ontologies, serving as the foundation of the Semantic Web for knowledge sharing, information extraction, and integration [106], crucial for achieving data integration and semantic interoperability. Ontologies may adopt a formal syntax or language for precise representation, such as RDF or OWL [107].

To support interoperability, Xu et al. presented an IoT-based system for medical emergency services to collect, integrate, and interoperate IoT data in healthcare [108]. For this purpose, a semantic data model was proposed, which can store and interpret heterogeneous IoT data uniformly, a feature particularly useful in real-time applications. A ubiquitous data accessing method (UDA-IoT) was designed to improve accessibility to data sources by acquiring and processing IoT data ubiquitously. This resource-based IoT data-accessing method works effectively in distributed heterogeneous environments for timely access to the data in mobile and cloud computing platforms. Similarly, the authors [66] proposed a semantic model based on the IoT platform (SM-IoT), which provides interoperability between data sources and medical devices, along with contract-based security policies for the confidentiality of patient's health data.

The Digital Future project is proposed by Pazienza et al. [80], combining Semantic Web services with SOA-based principles by using an IoE (Internet of Everything) platform. They worked on interoperability at the semantic level by using middleware components. Kotha et al. [109] proposed a study focused on improving interoperability in healthcare IoT devices. It proposes a solution using natural language processing (NLP) techniques, specifically BERT for string matching and Fuzzy Inference System (FIS) for data correlation. The study aims to enhance data communication efficiency among IoT devices in healthcare, not directly addressing cyberattack detection. The

proposed approach, tested with real-world data, achieved 85.71% accuracy and a processing delay of 0.46 seconds, demonstrating its potential to enhance IoT interoperability in healthcare.

To address the heterogeneity of different devices by integrating them and identifying and understanding their application programming interfaces (APIs) to collect their data, researchers [32] proposed a mechanism that constructs the ontologies of the various APIs from both known and unknown medical devices and identifies their syntactic and semantic similarity. Based on syntactic and semantic similarity, the final mapping has taken place to identify the nature of API methods for unknown medical devices. After recognizing the APIs of these devices, their data can be gathered through a generic data acquisition API, which is implemented for collecting the data from all devices. The mechanism was evaluated through a use case to identify the API method that provides the data of an unknown activity tracker, compared with the API methods of two activity trackers whose functionality was already known.

2.3.3.2 Cybersecurity Solutions for IoMT

Various researchers use techniques to identify malware, anomalies, and threats in medical IoTs and healthcare applications. Hodges et al, [110] emphasize security risks associated with internet-connected medical devices. They advocate for a unified database that combines medical equipment data with vulnerability information, leveraging the OVAL (Open Vulnerability Assessment Language) tool. OVAL is an open-source platform utilizing XML which evaluates system states against security risks. While transparent, providing users with insight into its operations, OVAL's primary limitation lies in its infrequent updates. This is exemplified by a notable delay in reporting CVE-2020-1029 in the National Vulnerability Database, resulting in a five-day lag in the OVAL repository.

In efforts to promptly detect vulnerabilities and cyberattacks while enhancing security mechanisms in the healthcare sector, researchers have developed models, frameworks, and mechanisms. Hei et al. [108] introduced a lightweight security scheme to counter resource depletion attacks. By utilizing Support Vector Machines (SVM) to analyze patterns generated by Implantable Medical Devices (IMD), the authors effectively mitigated malicious authentication attempts, thereby conserving significant IMD-related energy. The researchers achieved noteworthy accuracy in detecting unauthorized access attempts, with linear and non-linear SVM classifiers reaching 90% and 97% accuracy, respectively. However, the proposed scheme may encounter challenges if the smartphone serving as a classification mechanism is lost or forgotten by the patient, raising uncertainty about access authorization. Additionally, as the scheme was designed and tested solely on one type of IoT device, its applicability across various IoT types may be limited. Another place, by using intrusion detection-based system researchers [111], [112] identify and mitigate cyber-attacks in the IoMT environment.

2.3.4 Information Security Countermeasures in Medical Smart Homes

In the literature, some researchers deal with countermeasures for cyberattacks that occur in IoT networks for medical devices [83]. For instance, Yaqoob et al. [102] discussed the different solutions for security attacks in medical devices such as attestation-based architecture, isolation-based mechanisms, and data flow integrity. Ahmed et al., [113] developed an ECU-IOHT dataset for analysing attack

behaviour and providing countermeasures for the security community. This is a publicly available dataset for the healthcare domain where anomaly detection is performed using the nearest neighbour-based algorithms. Although medical smart homes are very attractive to cybercriminals, the medical IoT devices used in them often do not have publicly disclosed technical descriptions, making it challenging for adversaries to attack and security systems provided to protect them. In addition, the inclusion of configurations that are not available makes it difficult or infeasible to perform data aggregation and data fusion. The users, including patients, doctors, and healthcare providers have very limited interaction with these devices, and they are often unknown from a security perspective.

By building customized smart home settings, all objects might be fully understood and adequately secured, including devices, equipment, and connections. Persons involved in such a setting must be well-trained and familiar with technologies and devices. Furthermore, while different organizations make roadmaps to secure critical infrastructure from cyberattacks by providing standards and protocols, they are often informed and updated without having full access to technical specifications. In this scenario, the associated semantics cannot be captured in sufficient detail for querying and automated reasoning. Policymakers need to create models explaining how to implement the standards and protocols in such environments to protect sensitive data from cyber-criminals. There is also a need to develop organizational systems to support the current challenges such as security, privacy, scalability, interoperability, and data heterogeneity, along with business planning to improve cyber-resilience. Better cyber-resilience techniques and solutions can ensure patients and healthcare facilities trust medical IoT infrastructures. Through this, the adaptability and accessibility of medical devices and services can be enhanced, and positive outcomes for patients can be increased.

2.4 Key Technologies and Tools in Semantic Framework Development

This section discusses the various tools and technologies that are fundamental to defining and shaping the critical components of this study. It explains how each tool and technology contributes to the research, highlighting their roles and implications in enhancing the understanding of the core subjects under investigation.

2.4.1 Ontology Development

In the context of the semantic web, ontologies are critical components used to formally define terms to describe resources clearly and without ambiguity [101]. Ontologies represent the relationships between data and concepts, serving as the backbone of the semantic web [32]. Ontology languages such as RDF, OWL, and XML are employed to construct ontologies for various domains. For this purpose, various ontology formats, including RDF/XML (Resource Description Framework/Extensible Markup Language), OWL/XML (Ontology Web Language/XML), and OWL Functional Syntax, are used [104].

Ontologies are categorized into three types based on the application's perspective. The first category

is known as an upper ontology, which assists in defining and structuring terms and relationships within a particular domain by offering a foundational framework. In contrast, a reference ontology delineates the entities and relationships within a singular domain. The third classification is an application ontology, tailored for a specific context, serving as a fundamental repository to fulfill needs [114]. Further detail about ontology development is discussed in Chapter 4.

2.4.1.1 Tools for Developing Ontologies

To develop an ontology, various tools are used such as Ontolingua Server, OntoEdit, WebODE, Evonne, and Protégé among others [115]. The Ontolingua Server facilitates the storage, retrieval, and manipulation of ontologies created using the Ontolingua language. It provides a platform for managing ontological knowledge and supporting collaborative ontology development [116]. OntoEdit is an ontology editor that facilitates methodology-based ontology construction while fully leveraging its inferencing capabilities. Additionally, OntoEdit offers several features, such as a highly capable plug-in structure [117]. WebODE is an extensible ontology-engineering suite based on an application server, whose development started in 1999 and whose support was discontinued in 2006. The core of WebODE was its ontology access service, used by all the services and applications plugged into the server. The WebODE's Ontology Editor allowed editing and browsing WebODE ontologies and was based on HTML forms and Java applets [118]. Evonne is a web-based application built using Node.js and Express.js for the server-side implementation. On the client side, it utilize d3 for both views, while WebCola is employed for the force simulation and its settings within the ontology view [119]. One tool that is commonly used in the creation of ontologies is Protégé [120], which is an independent open-source tool that has an extensible architecture. Its main core is the ontology editor, and its functionality can be extended through the use of plug-ins for reasoning and querying.

1. **Resource Description Framework (RDF)**

   The Semantic Web (SW) provides a framework designed to enhance data sharing and reuse across different applications and organizations, a principle embodied by the Resource Description Framework (RDF). RDF is utilized to model knowledge resources, using Uniform Resource Identifiers (URIs) to identify these resources uniquely. The RDF Schema serves to define web-based resources, while SPARQL (Standard Protocol for RDF Query Language) is used for querying RDF graphs to extract information or data. These graphs are formatted to be machine-readable [121].

   In RDF[13], data is organized using a simple triple-based model, consisting of Subject, Predicate, and Object. This structure supports the exchange of data across the web, accommodating various data schemas. RDF data is organized into triples, which create a graph-based formalism for defining metadata. Each element is marked by a unique identifier (URI) and is serialized in XML (RDF/XML) to support data exchange through various textual formats, enhancing its accessibility and comprehensibility [122].

[13] https://www.w3.org/TR/rdf11-concepts/

2. **Web Ontology Language (OWL)** The W3C Web Ontology Language (OWL)[14] is a Semantic Web language designed to represent detailed and complex knowledge about entities, groups of entities, and their interrelations. Knowledge expressed in OWL can be utilized by computer programs to verify its consistency or to infer implicit information. OWL is a component of the W3C's Semantic Web technology stack, which also includes RDF, RDFS, SPARQL, and other standards [123].

   The Web Ontology Language (OWL) has gained popularity for formally defining classes and properties within a specific domain, typically to enable automated reasoning about domain instances. A notable feature of OWL DL is its formal semantics based on description logic, which are sound, complete, and relatively tractable. To utilize OWL DL's formal semantics, a reasoning system that enforces the language's axioms is required. Notable examples include the tableaux reasoners FaCT, Pellet, and RACER. [124].

   In 2017, the W3C established SHACL as a key standard for validating RDF data. This machine-readable language allows computers to handle validation tasks through "shapes" that must be verified against specific nodes in the graph, known as targets. A significant distinction between OWL and SHACL is that SHACL operates under the Closed-World Assumption (CWA), meaning it assumes that all true facts are represented within the graph, while the profiles of OWL are based on Description Logics (DLs) and make the Open-World Assumption (OWA). Intuitively, this means that the given data is only a partial description of the facts; missing data can also be true. While SHACL excels at validation, RDF and OWL are better suited for cases where complex reasoning, flexibility, and inferencing are more critical—likely aligning more closely with the objectives of the MIoT semantic model [125], [126], [127], [128].

3. **Protégé**

   Protégé 5.5.0 is a Java-based application tool developed by Stanford University used for constructing ontologies. The software features various tabs, including Classes, Object Properties, Data Properties, Individual Classes, DL Query, SPARQL Query, Semantic Web Rule Language (SWRL) tab, and OntoGraph. The protégé is the Class tab utilized to create class hierarchies, while object properties and data properties can be added based on the domain and scope of the project. These properties can have characteristics such as functional, Inverse, Functional, transitive, and symmetric [104].

   A protege is an invaluable tool due to its versatility and functionality in the realm of ontology development and knowledge representation. As an open-source platform, it provides a user-friendly environment for creating, editing, and managing ontologies. Its intuitive interface and extensive set of features make it accessible to both novice and experienced users in fields such as artificial intelligence, semantic web, and biomedical informatics. One of the key advantages of Protege is its flexibility in supporting various ontology languages and formats, including OWL, RDF, and XML [120]. This versatility enables users to work with different ontology standards and seamlessly integrate their ontologies with other tools and systems. Additionally,

[14] https://www.w3.org/OWL/

Protege offers powerful inference capabilities, allowing users to perform automated reasoning on their ontologies. This helps in identifying inconsistencies, inferring implicit knowledge, and validating ontology designs, ultimately enhancing the quality and reliability of ontological models [129].

2.4.1.2 Reasoning Mechanism

The Knowledge-Based Systems (KBSs) are computer programs developed from Artificial Intelligence research, designed to replicate aspects of human knowledge and expertise for performing tasks traditionally handled by human experts. Hence, a knowledge-based system consists of two core elements: a knowledge base and an inference engine. The knowledge base contains facts or information about the world, while the inference engine enables the derivation of new knowledge from the existing data. The most common manifestation involves IF-THEN rules, often coupled with either forward or backward chaining approaches [130].

Rule-based reasoning is a form of logic-based reasoning that uses a set of logical rules to make inferences and draw conclusions. In this method, knowledge is represented as rules, each comprising a set of conditions and corresponding actions. When the conditions of a rule are satisfied, the associated actions are executed.

There are two primary types of rule-based reasoning: forward chaining and backward chaining. Forward chaining starts with known facts and applies inference rules iteratively to derive additional information until a specific goal is reached. This process progresses from existing data toward conclusions, continuously adding new facts. It follows a bottom-up strategy, driven by the available data. In contrast, backward chaining begins with a desired end goal and works backward through the rules to identify supporting facts. It initiates by defining the desired outcome and then seeks out the necessary conditions to achieve it, following a top-down, goal-driven approach [131], [132], [133].

The quality and correctness of ontologies are crucial for effective semantic representation and knowledge sharing. Ensuring ontology quality requires addressing inconsistency and uncertainty in real-world applications. An inconsistent ontology contains errors or conflicts, leading to incorrect interpretation of some concepts and resulting in false semantic understanding. An uncertain ontology has probabilistic correctness. Ontology reasoning helps reduce information redundancy in the knowledge base and identifies conflicts in knowledge content.

Numerous reasoning engines are available for ontology models, including Jena[15], Fact++[16], Racer[17], HermiT[18], Pellet[19], and others [134; 135]. These reasoners possess several important attributes, including the inference algorithm, supporting logic, degree of reasoning completeness, implementation language, and other characteristics [134].

In this research, the Pellet reasoner is employed to evaluate the performance of ruleset generation and the consistency of the ontology. Pellet is an OWL-DL reasoner based on the tableaux algorithm

[15]https://jena.apache.org/documentation/inference/
[16]http://owl.cs.manchester.ac.uk/tools/fact/
[17]https://www.ifis.uni-luebeck.de/ moeller/racer/
[18]http://www.hermit-reasoner.com/
[19]https://www.w3.org/2001/sw/wiki/Pellet

that supports forward chaining reasoning. It is renowned for its extensive middleware, unique features, and strong performance. Pellet also implements several OWL-DL extensions, including a combination formalism for OWL-DL ontologies and preliminary support for OWL/Rule hybrid reasoning [30].

1. **Semantic Web Rule Language (SWRL)**

   In healthcare, declarative approaches are particularly effective for processes such as computer-aided decision-making or disease diagnosis and treatment. Despite the effectiveness, interoperability among existing rule-based systems remains limited. SWRL has emerged to improve interoperability from the Semantic Web perspective, offering a robust solution for enhancing communication among diverse systems [133], [136].

   Semantic Web languages provide a formal means to represent knowledge and facilitate information exchange. Some languages support Horn-like rules or First-order logic, enabling declarative programming. An example is the Semantic Web Rule Language (SWRL) [133]. SWRL combines the Web Ontology Language (OWL) and Rule Markup Language (RuleML), allowing users to define rules and logical constraints within the semantic web framework. This setup enhances reasoning, expressiveness, and inference capabilities in ontology-based systems [137], [138].

   SWRL is a powerful language for expressing rules in combination with OWL ontologies, and it has become a key component in semantic web applications. It's often used in conjunction with ontology reasoners and has been referred to as a 'de-facto' standard derived from the Protege SWRL Tab plugin. Apart from it, these rules are represented in FOL (First-Order Logic), and Propositional Logic. While these may not be formal standards set by a standards organization, their widespread use and acceptance in various applications have given them the status of de-facto standards within their fields. They are essential for the development of theories, applications, and tools that involve logical reasoning and knowledge representation.

   In SWRL, each rule consists of an antecedent (conditions that must be met) and a consequent (actions to be taken if the conditions are fulfilled), formulated as "antecedent (body) $\rightarrow$ consequent (head)." For instance, SWRL can express complex medical rules like the following:

$$\begin{aligned} &\text{Patient}(\texttt{?patient}) \land \text{hasCondition}(\texttt{?patient}, \text{Diabetes}) \land \\ &\quad \text{hasPrescription}(\texttt{?patient}, \texttt{?medication1}) \land \\ &\quad \text{hasPrescription}(\texttt{?patient}, \texttt{?medication2}) \land \\ &\text{hasDrugInteraction}(\texttt{?medication1}, \texttt{?medication2}) \rightarrow \\ &\quad \text{hasRisk}(\texttt{?patient}, \text{"Potential drug interaction"}) \end{aligned}$$

This rule identifies a patient (?patient) with Diabetes and checks for drug interactions between two prescribed medications (?medication1, ?medication2). If an interaction exists, the rule concludes that the patient is at risk of a "Potential drug interaction," allowing healthcare systems to automatically alert both patients and providers, thereby facilitating preventive measures.

2.4.1.3 Generative Artificial Intelligence (Gen AI)

Large language models have seen exponential advancements with transformer tools such as GPT-3, GPT-4, and ChatGPT. In June 2020, OpenAI, a leading AI research laboratory, launched the groundbreaking Generative Pretrained Transformer 3 (GPT-3) model [139]. This revolutionary NLP model employs deep learning to generate human-like text, offering myriad applications through its easy-to-use APIs. Following GPT-3, OpenAI introduced even more advanced and sophisticated multilingual NLP models, including GPT-4, ChatGPT-4, and the latest ChatGPT Plus launched in 2023 [140]. These models have significantly enhanced the capabilities and accessibility of natural language processing, driving innovation across various fields.

ChatGPT, a generative artificial intelligence (AI) chat machine developed by OpenAI, has been explosively stimulating worldwide discussion about its capabilities and limitations since its launch in November 2022 [141; 142]. Generative AI (GenAI) refers to a class of artificial intelligence models designed to generate new data that mirrors the patterns and characteristics of the data they were trained on. These models, such as Generative Adversarial Networks (GANs), have demonstrated remarkable versatility and have been used to create diverse forms of content, including images, text, and music, showcasing their broad applicability and potential to transform various industries [143; 144].

This revolutionary technology represents a significant leap in artificial intelligence research, offering numerous benefits and opening new avenues for innovation across various domains such as transportation [141], education [142] and healthcare [145]. The Internet of Medical Things (IoMT) plays an important role in healthcare, providing patient monitoring, assistance, and diagnosis both locally and remotely. As medical devices become increasingly interconnected and reliant on networked systems. This situation presents significant challenges in maintaining cyber-resilience across networks, especially concerning data security. As a result, patients' health could be compromised. Managing such systems requires continuous monitoring and partial automation. For this purpose, rules are generated to identify vulnerabilities and anomalies in the system with the help of formal logic.

Generative AI models learn patterns, structures, and relationships within input data and use this knowledge to create new, possible instances of data. This research utilizes generative AI models to evaluate the performance of rules developed to enhance security automation in the IoMT environment. These models are trained on provided rules and test use cases, enabling them to identify deviations from the norm and flag potential anomalies, vulnerabilities, and attacks.

2.4.1.4 Knowledge Graph

Google introduced the term "knowledge graph" in 2012 [146], [147] to describe the utilization of semantic knowledge to improve the quality of their search results. Knowledge graphs serve as a means to visualize knowledge resources and their associations. They can act as a valuable source of background knowledge for understanding user intent, supporting logical reasoning about knowledge and facts, and achieving semantic search generalization [148].

A knowledge graph is a semantic network that stores entities and their relationships in a graph format. Unlike traditional storage methods, the knowledge graph offers higher query efficiency. This efficiency is achieved through its ability to model complex interrelations between data points, allowing

for more sophisticated queries and faster retrieval of relevant information [149].

Furthermore, knowledge graph facilitate the integration and unification of heterogeneous data sources. They provide a structured framework that enables the merging of information from diverse domains, enhancing the richness and comprehensiveness of the data. This integrative capability is crucial for applications such as artificial intelligence, machine learning, and data analytics, where the quality and connectivity of data significantly impact performance.

1. SPARQL Query and SPARQL endpoint

   The RDF graphs are queried using a language called SPARQL (pronounced "sparkle" [150], [151]), stands for "SPARQL Protocol and RDF Query Language" or SPARQL Protocol. SPARQL is a standard query language and data access protocol designed particularly for handling RDF data models [121]. Here is an example of a SELECT statement to access data from an RDF model.

   ```
   SELECT DISTINCT ?s ?p ?o
   WHERE {
     ?s ?p ?o
   }
   LIMIT 100
   ```

   SELECT and WHERE are reserved keywords, while ?s indicates subject, ?p indicates predicate and ?o indicates object in triple format.

   SPARQL consists of two main components: a query language and a protocol. The query language aspect is fairly straightforward. Just as SQL is used to query relational data and XQuery is used to query XML data, SPARQL is used to query RDF data. RDF (Resource Description Framework) is a standard for representing data on the web, known as Linked Open Data [151]). However, SPARQL differs in a significant way: it was designed to operate not only on local databases but also over disconnected sources across a network [152]. Meanwhile, the protocol provides a way to convey SPARQL queries and updates from clients to SPARQL processors [153].

   A SPARQL endpoint A SPARQL endpoint allows users to send queries to a remote RDF dataset over the internet. This dataset may contain millions of triples, which are statements describing relationships between resources on the web. These resources can represent anything from people and places to various objects, all interconnected through linked data. [151]), [153]. In this study, GraphDB SPARQL endpoint is used to query and retrieve the information from the knowledge graph.

2.4.1.5 NVD, CVE and CVSS

The National Vulnerability Database (NVD) [154] is the U.S. government repository of standards-based vulnerability management data operated by the National Institute of Standards and Technology

(NIST)[20]. It serves as a comprehensive repository for identifying vulnerabilities in software across various computer systems. Among the most utilized sources of vulnerability information are the Common Vulnerabilities and Exposures (CVE) feeds. CVE serves as a worldwide database maintained collaboratively by security providers, developers, and researchers, harnessing the collective expertise to catalogue common vulnerabilities. With over 200,000 vulnerabilities indexed thus far, the contributions from these groups are integral to its function. Consequently, CVE plays a pivotal role in advancing security standards. Furthermore, the CVE data stream has established partnerships with numerous security providers globally [155].


```
{
  "cve" : {
    "data_type" : "CVE",
    "data_format" : "MITRE",
    "data_version" : "4.0",
    "CVE_data_meta" : {
      "ID" : "CVE-2023-0849",
      "ASSIGNER" : "cna@vuldb.com"
    },
    "problemtype" : {
      "problemtype_data" : [ {
        "description" : [ {
          "lang" : "en",
          "value" : "CWE-77"
        } ]
      } ]
    },
    "references" : {
      "reference_data" : [ {
        "url" : "https://vuldb.com/?id.221152",
        "name" : "https://vuldb.com/?id.221152",
        "refsource" : "MISC",
        "tags" : [ ]
      }, {
        "url" : "https://vuldb.com/?ctiid.221152",
        "name" : "https://vuldb.com/?ctiid.221152",
        "refsource" : "MISC",
        "tags" : [ ]
      } ]
    },
    "description" : {
      "description_data" : [ {
        "lang" : "en",
        "value" : "A vulnerability has been found in Netgear WNDR3700v2 1.0.1.14 and classified as critical. This vulnerability affects unknown code of the component Web Interface. The manipulation leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-221152."
      } ]
    }
  },
  "configurations" : {
    "CVE_data_version" : "4.0",
    "nodes" : [ ]
  },
  "impact" : { },
  "publishedDate" : "2023-02-15T22:15Z",
  "lastModifiedDate" : "2023-02-15T22:15Z"
}
```


Figure 2.3: A sample NVD CVE Json entry.

In the NVD database, each CVE is tagged with a publication date timestamp and a unique sequential number, such as CVE-2017-0144 [156], [157], [158]. Figure 2.3 displays a sample NVD CVE Json entry, illustrating key elements including CVE ID, version, description, publication date, and last modified date. This entry serves as a crucial reference point, providing trusted information to determine the timing and circumstances surrounding the emergence of various CVEs, both new and recurring, within any threat landscape.

Moreover, the NVD employs the Common Vulnerability Scoring System (CVSS) to evaluate the severity of vulnerabilities. Ranging from 1 to 10, the CVSS score assesses the potential impact of exploiting a vulnerability on attributes like confidentiality, integrity, and availability, alongside considering the attack vector and complexity [156], [158], [159].

[20]https://www.nist.gov/

2.5 Conducting a Scoping Literature Review

While researching the background literature for this thesis, it became clear that the specific knowledge and information that directly informed the emerging knowledge vectors for this thesis would depend upon a wide range of new and rapidly emerging knowledge. To ensure this knowledge was clearly understood and that clarity was based on both conceptual and technical reasoning, the literature review was expanded to include a scoping literature review, with the expressed purpose of defining the new knowledge area, identifying gaps in knowledge, and identifying the emerging elements of greatest interest and application.

In the early stages of this study, a literature review was conducted to gather preliminary insights into the domain of the Internet of Medical Things, including telehealth, remote patient monitoring, and aged care. This initial stage further focused particularly on IoT medical devices used in remote patient monitoring, examining different techniques and methods used to identify vulnerabilities and cyberattacks in this application. These diverse domains served as a foundation for investigating various approaches, such as Explainable AI, blockchain, mining-based, and reasoning-based approaches.

To make these searches optimal and efficient, a scoping review was conducted. It provided an overview and exploration of the existing literature related to the interdisciplinary research area of IoMT and cybersecurity. The scoping review identified and mapped the breadth and depth of the available research, including key concepts, methodologies, and gaps in knowledge. By conducting the scoping review, the researcher was able to establish a comprehensive understanding of the field, identify research gaps, and determine the novelty and contribution of their work within this context.

2.5.1 Vulnerability Detection for IoMT in Remote Patient Monitoring: A Scoping Review

Due to the rapid and ubiquitous development and acceptance of IoT, healthcare providers have changed their locational settings from solely based in clinics to extend more broadly into the reach of patients' domestic homes [48]. This IoMT focus extends to various medical devices and applications within the healthcare domain, such as any form of smartphones, surveillance cameras, wearable sensors, and actuators, that hold the capability to access IoT technologies [11], [34], [35], [36]. Medical IoT devices, specifically designed for patient monitoring and diagnosis, excel in their ability to collect, transfer, and interact with (near-) real-time data [51].

Nowadays, medical devices are more portable, connected through a network and with the capability to provide services to humans remotely. At the same time, these medical devices face security breaches due to a lack of standard protocols defined by regulatory bodies and manufacturers [160]. This trend is a significant element in understanding the importance of medical data generated from the home but also demonstrates the emerging critical need for smart home data and IoT data to form part of an inherently cyber-secure environment.

2.5.1.1 Summary of Scoping Review

This scoping review methodology was employed to explore the standards, protocols, and recommendations to find out the approach for gathering adequate information to define a research area. The initial step involved sourcing relevant literature was executed using content analysis. Given that IoMT is an emerging technology, it is constantly changing and therefore requires frequent updates. Additionally, given the limited available research in the new and emerging areas of interest here, (and the relatively short timeline), the approach taken was to consider both peer-reviewed scientific publications, research articles and conference proceedings for examination. The subsequent sections below provide the details of specific literature selection along with the aim of this review. There is an explanation of the method of searching different databases and developing uniquely targeted search strings. This scoping review also provides a literature review protocol that contains inclusion and exclusion criteria. The final assessment and analysis will be performed based on data extraction and data synthesis.

2.5.2 Scoping Review Method

This research followed the JBI (Joanna Briggs Institute) methodology for scoping reviews [161] is a structured approach for conducting scoping reviews, and a system which identifies the type of literature review design that is most aptly suited to map and summarize existing research on a broad topic to identify gaps in the literature, key concepts, and areas where further research may be needed. The JBI methodology provides a systematic and transparent way to conduct scoping reviews. Here are some key steps and components of the JBI methodology for a scoping review.

2.5.2.1 Eligibility Criteria and Sources

Table 2.1: Population, Concept, and Context (PCC)

Population, Concept, and Context	
Population	Remote patients
Concept	IoT devices using Network protocols such as Bluetooth or Wi-Fi
Context	Detection of vulnerabilities or cyberattacks on medical devices

This section *(Table 2.1 PCC)* examines studies related to IoMT or e-healthcare applications where remote patient monitoring and diagnosis have been done. In terms of concept, IoT devices are wearable or implantable in medical settings where remote monitoring has been done and their data is transferred through network communication protocols. For context, this research particularly focused on the detection of vulnerabilities and cyberattacks on medical devices. In this way, this methodology follows further these steps to conduct a scoping review.

2.5.2.2 Identifying the research question

The first step of the scoping review consisted of the identification of the aim of this study. One of the research questions for this study was:

RQ1: How can data be optimized to support cybersecurity posture of remote patient monitoring systems on the Internet of medical things (IoMT)?

RQ2: How can vulnerabilities be detected automatically within remote patient monitoring systems?

To answer these research questions, a scoping literature review was carried out. The main purpose of reviewing the literature was to discover information about the existing standards, rules and guidelines that have been established in the design and development of frameworks and models for improving the (cybersecurity posture of remote patient monitoring systems/Internet of medical things). For this purpose, different databases were searched by using search strings, and relevant literature was chosen to answer the given research question.

2.5.2.3 Databases and search strategy for review

Nowadays, electronic databases are the first place to search literature. To ensure the inclusion of high-quality research, this study primarily relied on reputable sources such as SpringerLink, IEEE Xplore Digital Library, ACM Digital Library, Scopus and Science Direct.

This study utilized five attributes of the search syntax:

1. TITLE-ABS-KEY: This attribute entails searching for the selected keywords within the title, abstract, and keywords of the research papers/articles.
2. AND: This operator requires the presence of both keywords in the searched item i.e., IoMT and cyberattacks.
3. OR: This operator necessitates the presence of at least one of the terms in the searched item i.e., vulnerabilities or cyberattacks.
4. NOT: This operator excluded the terms and keywords from the literature.
5. Year: This attribute allowed us to specify the publication period range to align with the topic's timeline.

To refine the search for relevant articles and narrow down the results, his study utilized specific criteria (C) for the search strings, which included:

1. C1: Semantic Modeling AND Knowledge Graph AND Vulnerability OR Cyberattack AND IoMT
2. C2: Automated Reasoning AND IoMT NOT Machine Learning NOT Deep Learning
3. C3: Rule-based Reasoning AND cyberattacks OR vulnerability AND IoMT
4. C4: IoMT AND cyberattack OR Vulnerability AND knowledge graph

Initially, the titles and abstracts of the relevant literature from each of the databases were found and analyzed. The next step involves screening the reference lists for full-text screening using exclusion criteria. The databases are used to search for articles, conference proceedings, and grey literature, as shown in the table 2.2.

Table 2.2: Search Strings and Results

Search Strings and Results		
Database	**Search Strings**	**No. of Articles (2018-2023)**
SpringerLink	C1: Semantic Modeling AND Knowledge Graph AND Vulnerability OR Cyberattack AND IoMT	10 (Only review and Journal Articles)
	C2: Automated Reasoning AND IoMT NOT Machine Learning NOT Deep Learning	6 (All types of articles in Computer Science and Engineering disciplines)
	C3: Rule-based Reasoning AND cyberattacks OR vulnerability AND IoMT	11 (Only Review and Journal articles)
	C4: IoMT AND cyberattack OR Vulnerability AND knowledge graph	362 (Only Journal articles in Computer Science)
IEEE Xplore Digital Library	Semantic Modeling AND Knowledge Graph AND Vulnerability OR Cyberattack AND IoMT	24 (Only Journal articles and Conference Proceedings)
	Automated Reasoning AND IoMT NOT Machine Learning NOT Deep Learning	8 (All results)
	Rule-based reasoning AND cyberattacks OR vulnerability AND IoMT	13 (Only Journal articles)
	IoMT AND cyberattack OR Vulnerability AND knowledge graph	20 (Only journals)
Science Direct	Semantic Modeling AND Knowledge Graph AND Vulnerability OR Cyberattack AND IoMT	253 (Only review articles in the Computer Science and Engineering Field)
	Automated Reasoning AND IoMT NOT Machine Learning NOT Deep Learning	6 (All types of articles in all disciplines)
	Rule-based reasoning AND cyberattacks OR vulnerability AND IoMT	11 (All types of articles in all disciplines)
	IoMT AND cyberattack OR Vulnerability AND knowledge graph	27 (All types of articles in all disciplines)
Scopus	Semantic Modeling AND Knowledge Graph AND Vulnerability OR Cyberattack (6 documents) AND IoMT	0 (All articles and Reviews are included in Computer Science)
	Automated Reasoning AND IoMT NOT Machine Learning NOT Deep Learning	1 (All types of articles in Computer Science)
	Rule-based reasoning AND cyberattacks OR vulnerability AND IoMT	0 (All document types in Computer Science)

Continued on next page

Table 2.2 – continued from previous page

Database	Search Strings	No. of Articles (2018-2023)
	IoMT AND cyberattack OR Vulnerability AND knowledge graph	2 (Only research articles and review articles in Engineering and Computer Science and Math)
ACM Digital Library	Semantic Modeling AND Knowledge Graph AND Vulnerability OR Cyberattack AND IoMT	9 (Only Journals)
	Automated Reasoning AND IoMT NOT Machine Learning NOT Deep Learning	1 (All publications)
	Rule-based reasoning AND cyberattacks OR vulnerability AND IoMT	17 (Only journal articles)
	IoMT AND cyberattack OR Vulnerability AND knowledge graph	13 (Only Journal and research articles)

2.5.3 Study Selection

Two reviewers performed the title, abstract, and full-text screening independently in adherence to the inclusion criteria. The criteria for exclusion with additional refinement of exclusion reasons take place during the full-text screening process.

2.5.3.1 Inclusion Criteria

Table 2.3 shows the inclusion criteria for the study selection. It mainly includes the domain of research, the models and frameworks developed in this domain, and whether cyberattack and vulnerability detection are performed.

Table 2.3: Inclusion Criteria

Inclusion Criteria	
No.	**Description**
1	The papers are in English Journal or conference proceedings or published thesis.
2	Presents a survey or review of the IoMT framework, models, or applications for remote monitoring systems.
3	Discuss the cyberattacks and vulnerabilities in the Internet of medical things or healthcare.

Continued on next page

Table 2.3 – continued from previous page

No.	Description
4	Knowledge Graph for vulnerability/cyberattack detection specifically in healthcare/IoMT.
5	The articles are not older than the last five years, such as 2018-2023.
6	Automated reasoning by rule-based techniques.

2.5.3.2 Exclusion Criteria

This section outlines the exclusion criteria for the literature, such as papers that are not in English or not peer-reviewed. Only medical devices are considered, excluding other IoT devices like smartwatches or smartphones. Knowledge graph representation in other domains is also excluded, as shown in Table 2.4.

Table 2.4: Exclusion Criteria

Exclusion Criteria	
No.	**Description**
1	Not written in the English Language.
2	Not published in peer-reviewed journals or conferences.
3	Papers covering medical devices such as mobile phone sensors or smartwatches.
4	Papers on Knowledge Graph for vulnerability/cyberattack detection in other domains such as IoT networks.

2.5.4 Data Extraction

In the process of data extraction from included studies for a literature review, our approach to extracting information from selected studies involves an analysis of several critical aspects:

- **Publication Details:** This includes the study's title, authors, year of publication, and the journal or conference in which it was published. Understanding the source helps in assessing the credibility and relevance of the research.
- **Methodology:** An investigation of the research methods employed in each study, such as qualitative analysis, quantitative experiments, case studies, surveys, etc. This helps in understanding how the research was conducted and the validity of its findings.

- **Techniques for Detecting Vulnerabilities or Cyberattacks in IoMT:** Special attention is given to the specific techniques, algorithms, or frameworks used in the studies for identifying and addressing cybersecurity threats. This included machine learning models, heuristic methods, intrusion detection systems, and blockchain.
- **Knowledge Representation and Reasoning Techniques:** This involves analyzing how the studies process and interpret data, including the logic and reasoning applied, and how they represent and manage knowledge within the study in a semantic way.
- **Key Findings:** Each study's main results, conclusions, and significant discoveries are summarized. This includes understanding what new insights or contributions the study makes to the field of cybersecurity in IoMT/healthcare.
- **Contributions to the Field:** An evaluation was undertaken of how each study contributes to the broader field of cybersecurity related to healthcare. This included advancing theoretical understanding, developing new techniques, and the provision of empirical data.
- **Study Challenges and Limitations:** The identification and understanding of the challenges faced during the study and any limitations in its scope, methodology, or findings was crucial. This assisted in assessing the reliability of the study and understanding the context in which the findings should be interpreted.

Through this detailed approach, the aim is to gain a comprehensive understanding of the existing research landscape in healthcare, specifically regarding the Internet of Medical Things for remote monitoring to detect vulnerabilities or cyberattacks. This analysis highlights both the progress made and the areas that need further exploration. This thorough analysis was fundamental in building a sophisticated understanding of the field and identifying future research directions.

2.5.5 Results

2.5.5.1 General Overview

Figure 2.4 outlines the study selection process for this review. Initially, 794 sources were screened for eligibility, with 279 being discarded after title and abstract evaluation. The full-text screening phase involved 68 records, out of which 37 were excluded. Consequently, 31 papers were selected for inclusion in the review. Details of the included studies are available in Appendix B. The primary reason for study exclusion post-full-text screening was 'vulnerability/cyberattack detection in IoMT by using automated reasoning'. This referred to studies not related to IoMT settings for remote monitoring patients. Most of the literature addresses only those vulnerabilities/cyberattacks related to IoT networks, which is not the focus of this study.

Figure 2.5 represents the distribution of articles used in a scoping review. The chart segments reflect the proportion of articles sourced from different academic databases such as SpringerLink, IEEE Xplore, ACM Digital Library, Scopus, and ScienceDirect. Each segment's size indicates the

relative number of articles drawn from each database, providing a visual summary of the databases' contribution to the review.

The review's overview is illustrated in Figure 2.6, showcasing publication years (2018-2023). The years 2022 and 2023 show a significant rebound, with 2023 showcasing the highest number of publications compared to the previous years. The bar chart shown in Figure 2.7. reflects the number of studies utilizing various themes or technologies. The categories from left to right are Ensemble Learning and Fog-Cloud (EL and FC), Machine Learning and Deep Learning (ML and DL), Federated Learning (FL), Blockchain, Hybrid and others. The 'Hybrid and others' category has the highest number of studies, indicated by the tallest bar, while 'EL and FC' have the fewest, shown by the shortest bar.

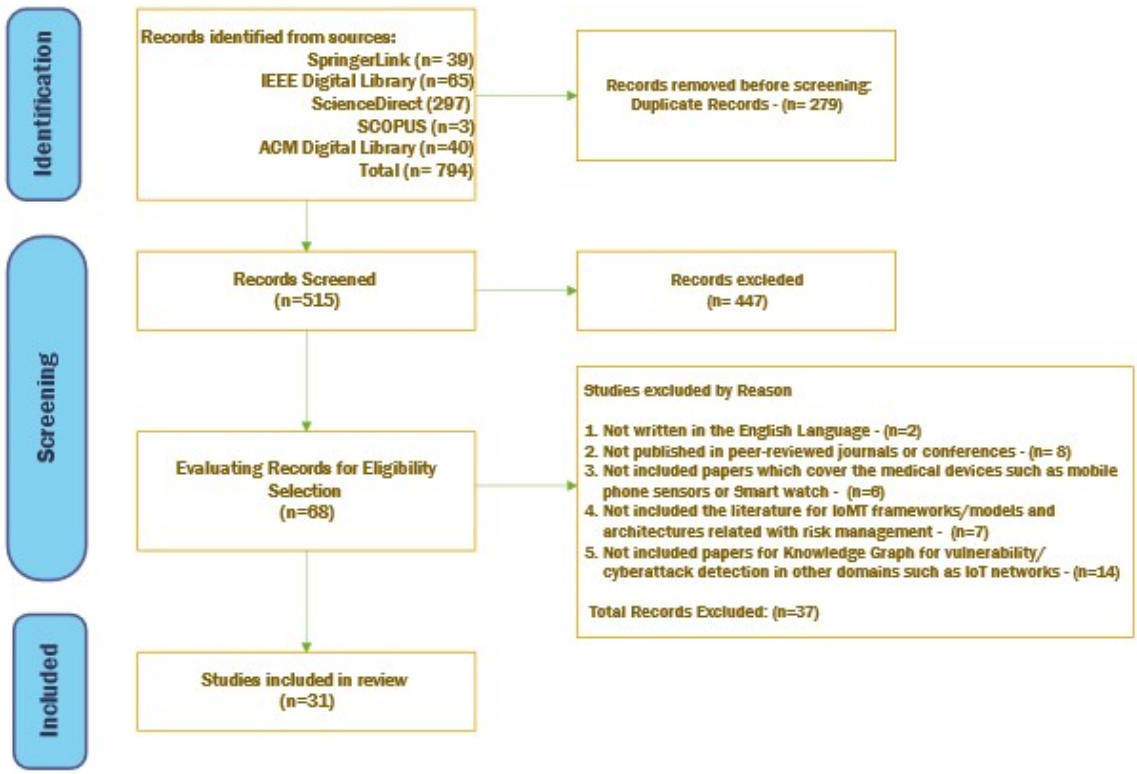
Identification
Records identified from sources:
SpringerLink (n= 39)
IEEE Digital Library (n=65)
ScienceDirect (297)
SCOPUS (n=3)
ACM Digital Library (n=40)
Total (n= 794)
Records removed before screening:
Duplicate Records - (n= 279)
Screening
Records Screened
(n=515)
Records excleded
(n= 447)
Evaluating Records for Eligibility
Selection
(n=68)
Studies excluded by Reason
1. Not written in the English Language - (n=2)
2. Not published in peer-reviewed journals or conferences - (n= 8)
3. Not included papers which cover the medical devices such as mobile phone sensors or Smart watch - (n=6)
4. Not included the literature for IoMT frameworks/models and architectures related with risk management - (n=7)
5. Not included papers for Knowledge Graph for vulnerability/ cyberattack detection in other domains such as IoT networks - (n=14)
Total Records Excluded: (n=37)
Included
Studies included in review
(n=31)

Figure 2.4: PRISMA Study Selection Process [8], [9], [10] .

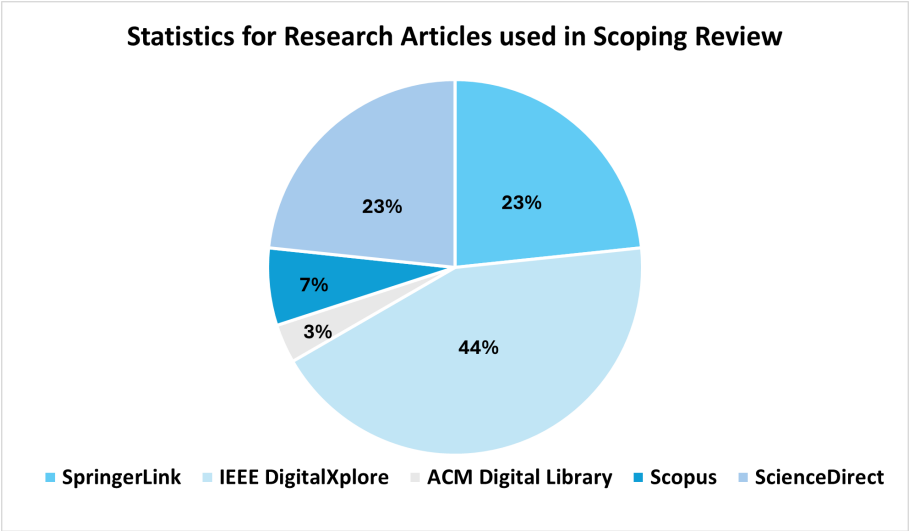

Figure 2.5: Statistics of research articles selected for Scoping Review.

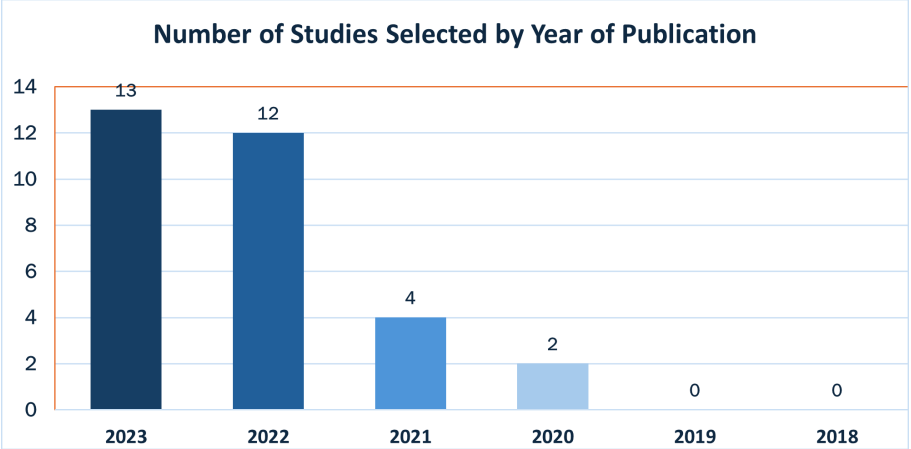

Figure 2.6: Included Studies by Year of Publication.

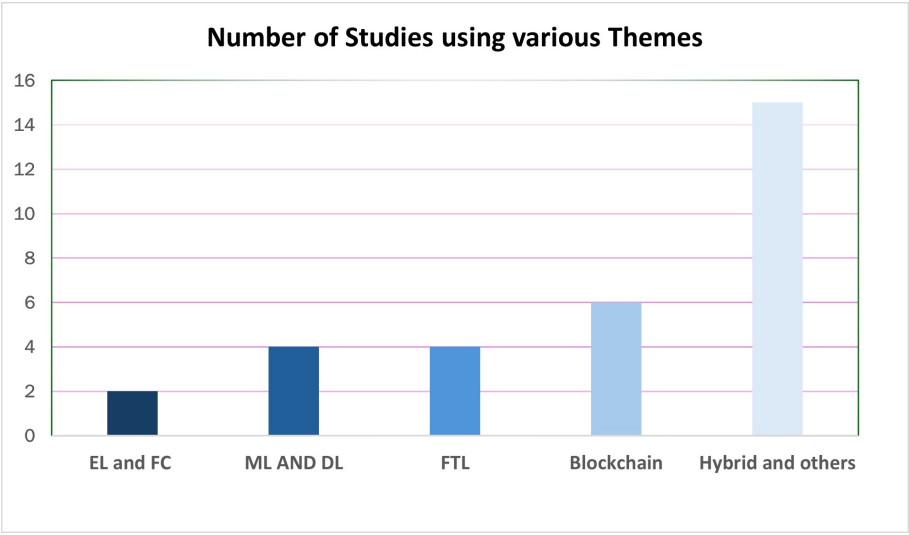

Figure 2.7: Included Studies by Technology used in IoMT for vulnerability/cyberattack detection.

The other categories have varying numbers of studies, with Blockchain having slightly more studies than 'ML DL' and 'FL'. The types of methodologies (qualitative, quantitative, and mixed methods)

are shown in Figure 2.8. It describes 39% of the studies used qualitative methods, the largest number of studies used in this scoping review. Quantitative methods were utilized in 32% of the studies, making it the second-largest segment. Mixed methods were employed in 29% of the studies, this visual representation indicates a balanced use of different research methodologies in this review.

2.5.5.2 Vulnerability and cyberattack detection in IoMT

This scoping review followed a qualitative synthesis approach, and it summarized, compared, and contrasted the characteristics and findings of the selected studies based on 5 themes. It explored the relationships between the findings and discussed their relevance and applicability to the research questions. The qualitative synthesis also involved an analysis of the strengths and weaknesses of the body of evidence, focusing on identifying gaps in the evidence and providing recommendations for further research.

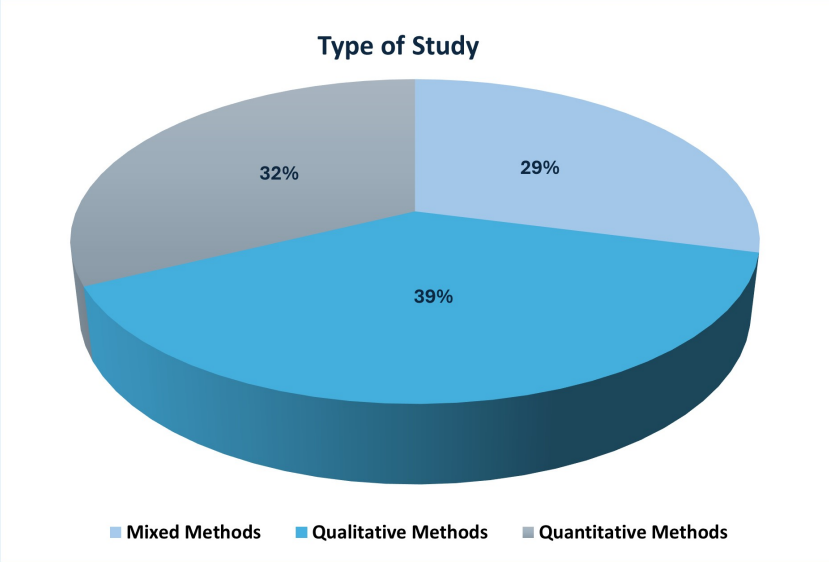

Figure 2.8: Included Studies by Technology used in IoMT for vulnerability/cyberattack detection.

a. ***Ensemble Learning and Fog-Cloud Architecture***

The work by Khan et al. [162] makes a significant contribution by discussing a secure ensemble learning-based fog-cloud approach for cyberattack detection in IoMT. This approach addresses security issues in IoMT networks caused by cyberattacks, offering a solution that utilizes ensemble learning and fog-cloud architecture. It is evaluated using the telemetry datasets of the IoT and IIoT sensors (ToN-IoT) dataset, with results showing a 4% improvement in precision over baseline approaches. This indicates the approach's high effectiveness in detecting cyberattacks in IoMT networks. The proposed IoMT-based solution can be deployed as Infrastructure as a Service in the cloud and Software as a Service in the fog, making it scalable and accessible to a wide range of healthcare providers. This work promotes potential improvements in the security of IoMT networks and enhances the quality of patient care in healthcare systems.

The methodology described in this research included a simulation-based evaluation of the proposed approach using the NS-3 simulator. The challenges faced in this research included the

lack of publicly available datasets for IoMT cyberattacks, which made it difficult to evaluate the proposed approach. Another challenge was the limited computational resources available for the simulation-based evaluation. One of the weaknesses of this research is that the proposed approach was evaluated using a simulated environment, which might not accurately reflect the real-world performance of the approach. Additionally, the proposed approach may not be effective against new and unknown cyberattacks that have not been included in the training dataset.

There is a growing body of research in support of the security of Internet of Medical Things (IoMT) networks, that highlights increased vulnerability to cyber-attacks, (as demonstrated by the 2018 ransomware attack on an Indiana hospital system). To achieve this, the authors Kumar et al., [111] proposed a cyber-attack detection framework that integrates ensemble learning with a fog-cloud architecture. This study focuses on designing an efficient cyber-attack detection framework to identify and mitigate threats in IoMT networks. The ensemble learning approach forms the core of this framework, combining Decision Tree, Naive Bayes, and Random Forest as first-level learners, with XGBoost for further classification. The proposed deployment architecture uses Software as a Service (SaaS) at the fog side and Infrastructure as a Service (IaaS) at the cloud side, addressing the dynamic and distributed nature of IoMT networks. The research stands out by utilizing the ToN-IoT dataset, collected from a heterogeneous and large-scale IoT network, overcoming the limitations of traditional datasets like KDD CUP99 or NSL-KDD that lack modern IoMT-based attacks.

The key challenges addressed in this research have included the design of a distributed security framework for the dynamic IoMT environment, creating a mechanism for analyzing large data volumes generated by IoMT devices, and developing an effective Intrusion Detection System. While the paper provides a comprehensive approach to IoMT security, it does not explicitly detail its limitations, which could include the evolving nature of cyber threats and the challenges in widespread implementation across diverse IoMT platforms.

b. ***Machine Learning (ML) and Deep Learning (DL) Methods***

Radoglou-Grammatikis et al. presented multiple research studies in his work in [163], [164]. Both research works dive into the complexities and security implications of the Internet of Medical Things (IoMT) within the healthcare system and tackle IoMT security challenges. In terms of IoMT and security concerns, the first proposed work highlights the swift evolution of IoMT and the integration of smart medical devices, spotlighting advantages such as remote medical assistance and real-time monitoring. It placed a broader focus on the overall impact of IoMT on healthcare, addressing associated cybersecurity and privacy issues. When it comes to protocols and technologies, the authors introduce an Intrusion Detection and Prevention System (IDPS) using Machine Learning (ML) and Deep Learning (DL) methods for HTTP and Modbus/TCP.

Furthermore, an active learning approach for IDPS had proposed and demonstrated efficiency against specific cyberattacks, it emphasizes active learning for re-training classifiers. The second

work placed a greater emphasis on addressing cybersecurity concerns related to the IEC 60 870-5-104 protocol in industrial healthcare systems. This work introduces an IDPS leveraging ML and Software-Defined Networking (SDN) technologies and quantitative threat model and an IDPS designed to automatically address IEC 60 870-5-104 cyberattacks using ML and SDN technologies.

DeepCAD, [165] is a framework that features a stand-alone deep neural network (DNN) model, uniquely integrated with anomaly detection rules. This integration is designed for effective classification and anomaly detection in Smart Healthcare Systems (SHS) focused on the Internet of Medical Things (IoMT) network. This research involves training the DNN using the Pima Indians Diabetes and Parkinson datasets, incorporating modified loss functions to enhance the model's ability to identify out-of-distribution samples as anomalies. Although its advanced approach, the framework highlights several challenges in terms of complexities, adapting to new and evolving cyber threats and the resource-intensive nature of deploying advanced DNN models in a dynamic cybersecurity environment.

Ravi [166] developed a sophisticated network intrusion detection system for smart healthcare systems using deep learning techniques. The system employs a multidimensional attention-based deep learning approach to enhance the accuracy of intrusion detection by analyzing network payloads. This method addresses challenges in feature extraction and improves the robustness of the detection system against network attacks. Future work suggested in the study involves refining this deep learning model to increase its effectiveness in detecting a wider range of network attacks which is crucial for ensuring robust security in the increasingly interconnected and vulnerable smart healthcare enterprise systems.

c. ***Federated Learning, AI and Explainable AI***

Federated Transfer Learning is used in developing intrusion detection systems (IDS) for enhancing cybersecurity in healthcare systems. In this regard, Otoum et al., [112] present a novel approach to improving cybersecurity in healthcare systems by proposing a Federated Transfer Learning-based Intrusion Detection System (IDS) for the Internet of Medical Things. The IoMT encompasses medical devices and applications connected through the internet, raising concerns about the security of patient data, particularly with the increasing frequency of cyberattacks. The proposed model utilizes Deep Neural Network (DNN) algorithms, employing federated transfer learning to build a global model collaboratively with edge devices, preserving data privacy. The study evaluates the model's performance using the CICIDS2017 dataset and demonstrates its effectiveness in terms of accuracy, detection rate, and average training time. The results suggest that the proposed model outperforms traditional centralized learning schemes, showcasing its potential for securing healthcare-connected devices in the evolving landscape of the IoMT.

The research proposed by Rahman et al., [167] focuses on Federated Learning (FL), Artificial Intelligence (AI), and Explainable AI (XAI) in smart healthcare systems. It aimed to improve intelligent healthcare systems by integrating these technologies to enhance data privacy, security, and system efficiency. The study explored the state-of-the-art in FL and AI, addressing challenges

like security, privacy, and reliability in healthcare systems. For this purpose, they are analyzing FL and AI applications, their integration, and performance in healthcare contexts. Further, they are exploring areas like AI with blockchain for security, FL in data science, and its application in various sectors like smart industrial IoT and big data analytics. They also look towards future advancements, including the application of AI in areas like blockchain and data science, aiming to further revolutionize healthcare management through these emerging technologies.

The research presented by Kulshrestha et al, [168] focuses on Federated Learning (FL), Artificial Intelligence (AI), and Explainable AI (XAI) in the context of intelligent healthcare. The primary aim was to address vulnerabilities and challenges in traditional healthcare systems that relied on centralized data sharing. By integrating FL, AI, and XAI, the research demonstrated a shift towards a decentralized model where multiple agent collaborators can communicate efficiently without the need to transfer raw data. This approach exemplified a way to minimize several limitations of the current healthcare systems and offers a thorough analysis of FL applied to AI for smart healthcare applications.

The research also highlighted several limitations and challenges in this area. These include privacy issues, difficulties in aggregating user data from different sources, the potential failure of cloud systems in personalized settings, and the sensitivity of healthcare data. Additionally, it pointed out the absence of an FL-based production-ready approach and the challenges related to data access policies and security concerns. The suggested future work was aimed at leveraging FL for various solutions, such as a blockchain and FL-based system to preserve privacy in the network, and a client-central module for real-world application. This system offered a precision-based method that was designed to cater to the needs of different patient groups, including those who prefer hospitalization and those who do not.

The work of Cartwright [169] highlighted the increasing frequency and impact of cyberattacks in the healthcare sector, particularly with the adoption of Internet of Things (IoT) devices and the rise of the Internet of Medical Things (IoMT). These technological advancements, combined with the COVID-19 pandemic, have significantly increased the vulnerability of healthcare systems to cyber threats. Although this research does not outline a specific experimental methodology, it provides a comprehensive review of the cybersecurity landscape in healthcare. The study included an analysis of various data breaches, the role of human error, and the impact of emerging technologies like AI in patient care, which bring both benefits and risks.

This research discusses the general landscape of cybersecurity in healthcare, including the risks posed by AI and the challenges brought by the COVID-19 pandemic. It emphasized the need for improved security measures and awareness but did not specify techniques for detecting cyberattacks or vulnerabilities. The paper's limitations mainly revolve around its scope. It primarily provided an overview of the current state of cybersecurity in healthcare and the associated risks but did not propose specific technological solutions or detailed methodologies for combating these challenges. The focus of this study was on raising awareness and calling for regulatory and funding changes to improve healthcare cybersecurity.

d. ***Blockchain Technology***

The survey paper by Almalki [170] focused on analyzing current state-of-the-art blockchain technologies and their applications in IoT-based healthcare systems. It acknowledged the diversity in both the dimensions of existing blockchain approaches and the requirements of IoT-based healthcare applications. The study showed a method to solve a gap in this area of research by thoroughly investigating how blockchain is being integrated into various IoT disciplines, particularly in the health sector. It also showcased the potential uses of blockchain in healthcare, highlighting both the challenges and future directions for its development.

The main limitations included unresolved security issues like hostile attacks and authentication challenges, ongoing issues with blockchain delay, and a lack of in-depth performance evaluation of the system. Additionally, the research did not conduct simulations to assess performance. As a result, it failed to provide detailed descriptions of blockchain settings and configurations. The future work in this area looked at improving the ubiquity of IoT services and enhancing system performance and security to meet the demands of emerging network technologies like 5G. This involves developing solutions for key Blockchain of Things (BCoT) network problems, such as resource scheduling, system management, and networking optimization. This research identified challenges in handling the massive amount of data expected from IoT devices streaming to the blockchain network, which could render traditional data analytics and processing methods ineffective.

The research proposed by [171] aims to improve smart healthcare monitoring systems by implementing blockchain technology. This is to enhance security and privacy in IoT-based healthcare systems, particularly in managing electronic health records (EHRs). The proposed framework uses blockchain to ensure data confidentiality and integrity. However, the research faces limitations, including unresolved security challenges and the need for more advanced blockchain development in healthcare contexts. Future work will concentrate on achieving scalability in blockchain applications, establishing universal standards for its adoption in healthcare, and bridging the knowledge gap about blockchain among healthcare professionals.

Nguyen et al. [96] present a healthcare architecture aimed at enhancing the efficiency and security of Internet of Medical Things (IoMT) networks. It integrates mobile-edge computing (MEC) and blockchain for efficient data offloading and sharing in distributed hospital networks. The authors propose a privacy-aware data offloading scheme and a blockchain-enabled data sharing scheme. These methods aim to enhance Quality of Services (QoS), privacy, and security in Internet of Medical Things (IoMT) networks. introduces a pioneering architecture aimed at enhancing the efficiency and security of Internet of Medical Things (IoMT) networks. It integrates mobile-edge computing (MEC) and blockchain to improve data offloading and sharing in distributed hospital networks. The approach focuses on improving Quality of Service (QoS), ensuring data privacy, and bolstering network security. The results demonstrate significant advancements in QoS, data privacy, and security, outperforming existing systems.

Some challenges and limitations are highlighted by the authors such as the complexity of real-

world deployment, scalability issues, and ensuring system reliability. Future work suggests exploring more efficient blockchain mechanisms, optimizing data offloading and sharing processes, and conducting extensive trials to validate the system's effectiveness in diverse healthcare settings. This forward-looking approach highlights the need for continuous development and testing in the evolving field of IoMT cybersecurity.

The research presented by Wazid et al., [35] focuses on proposing a blockchain-enabled security solution called BACKM-EHA for IoMT-based E-healthcare applications. The authors conducted a literature review of related existing schemes in the domain, and identified various research challenges such as scalability, energy efficiency, antenna design, interference mitigation, QoS, reliability, security, and privacy. They used a system model consisting of a network model and a threat model to design and implement BACKM-EHA. The proposed solution involves various phases such as registration, authentication, authorization, and revocation. The authors provided a formal security evaluation of their scheme to prove its security against various potential attacks. They also compared the proposed BACKM-EHA with other related existing schemes and demonstrated its impact on important performance parameters. BACKM-EHA provides a secure access control and key establishment between the body sensors and the personal server, and a secure key management between the personal server and the cloud server. It also presents a mechanism for the implementation of a "blockchain of healthcare data" over the cloud servers, which secures the entire communication between the body sensors, personal servers, and cloud servers. The authors provided a formal security evaluation of their scheme to prove its security against various potential attacks. The proposed solution has the potential to enhance the security and privacy of IoMT-based E-healthcare applications, which is crucial for the protection of sensitive patient data.

Some of the challenges faced by the authors include the complexity of the proposed solution, the need for a blockchain infrastructure, and the potential impact on system performance. One of the weaknesses of the proposed solution is that it may not be suitable for all types of IoMT-based E-healthcare applications, as it requires a certain level of technical expertise and infrastructure. Additionally, the proposed solution may not be cost-effective for small-scale healthcare providers.

The researchers [172] focused on enhancing the security of medical data within Smart Healthcare Systems (SHSs) by leveraging blockchain technology in the context of the Internet of Medical Things (IoMT). The study needs to ensure the confidentiality, integrity, and availability of sensitive Electronic Health Records (EHRs). In this regard, the research develops a framework integrating IoMT technology with cybersecurity, interoperability, and Big Data considerations. The methodology involves the development of a technical architecture for blockchain in SHSs, the creation of smart contracts for secure medical data processing, and an open data exchange format for EHRs based on a nested tree structure. The study also explores consensus algorithms for blockchain like Proof-of-Work (PoW) and Proof-of-Stake (PoS), and establishes an access control matrix to define system rights. Empirical testing and cybersecurity assessments are conducted using methods recommended by ENISA and NIST to identify and mitigate potential threats and vulnerabilities.

The complexity of cybersecurity in healthcare, especially in managing the vast and varied data of SHSs, presents a significant problem. Implementing blockchain technology while maintaining the balance of data integrity and confidentiality is a key challenge. Ensuring interoperability among diverse healthcare system components and standardizing data exchange formats add to the complexity. Additionally, securing the blockchain network in a decentralized and distributed environment against potential threats is crucial. The authors claim to focus on further refining the blockchain architecture for healthcare, optimizing smart contracts, and exploring more advanced consensus algorithms for enhanced network security and performance.

Kumaresan M. et al., [173] focus on enhancing the security and privacy of smart healthcare systems through the integration of blockchain technology, the Internet of Things (IoT), and 5G networks. This study involves a comprehensive review and analysis of existing technologies and their applications in healthcare, focusing on how their integration can improve security and privacy. This work involves the use of cryptographic concepts to secure and connect data blocks within these integrated technologies. They developed a framework and risk model for smart healthcare to showcase how the integration of these technologies can enhance healthcare delivery while addressing security and privacy concerns.

This research also identifies several challenges in healthcare security and privacy, including the complexity of implementing such an integrated system, ensuring data privacy and security, and managing risks associated with adopting new technologies. Further development of specific guidelines and best practices for the security framework implementation in various healthcare systems and adapting to evolving security threats in the smart healthcare industry is also discussed.

e. ***Hybrid Models and Integrated Approaches***

Mahmood et al., [174] conducted a Systematic Literature Review, which focuses on developing a security model for the Internet of Medical Things (IoMT) to address security threats, attacks, issues, and challenges. The methodology involves a systematic literature review (SLR), analyzing major security models, and conducting an extensive meta-analysis to prioritize risks. The proposed model includes a Python-based interface for identifying, prioritizing, and automatically controlling threats. That SLR is based on six research questions related to IoMT, security issues like threats, attacks, their architectures, and frameworks. Further, they used search strings, keywords, inclusion, and exclusion criteria and finalised 127 articles from seven different sources i.e., IEEE Xplore Digital Library, ACM Digital Library and more.

However, this article acknowledges the need for continuous improvements and updates to the security model in response to evolving threats in the IoMT industry. Future work suggested involves developing more specific guidelines and best practices for implementing the security framework in various IoMT systems and addressing the rapidly evolving security threats facing the IoMT industry.

Weber et al., [58] investigate the current state of research in detecting attacks on medical devices in hospitals and clinics, focusing on the challenges of hospital networks, attached medical

devices, and the variety of protocols used by these devices. The methodology used is a structured literature review (SLR) following the guidelines by Kitchenham et al. for SLRs in software engineering. Six research questions were developed to structure the review, covering aspects such as detection approach, location, included features, adversarial focus, utilized datasets, and intrusion prevention.

The researchers discuss the heterogeneity of devices, diversity of connectivity types, and the variety of terminology in medical cyber-physical systems (MCPS) as challenges they face. These challenges make it difficult to have central management of devices from assorted manufacturers and to fulfil the different connectivity requirements of different devices. Additionally, the lack of suitable datasets for training and testing algorithms led to the development of testbeds consisting of various medical devices. The paper suggests examining the special conditions of hospital networks and the MCPS deployed within them as future work. Additionally, creating MCPS-specific datasets, supporting activities aimed at standardization in this area, exploring the use of medical context for attack detection, and intensifying efforts for MCPS-tailored intrusion prevention. This future work is aimed at addressing the emerging threat landscape, improving IT security in hospitals, and protecting patient health.

Ghourabi A., [175] presents a novel approach to enhance cybersecurity in healthcare, particularly targeting the Internet of Medical Things (IoMT). The author develops a robust security system that can effectively detect and mitigate a wide range of cyber threats, including intrusions and malware, in healthcare settings. The methodology involves a hybrid model that combines an intrusion detection system using a LightGBM model and a BERT-based Transformer model for classifying network activities, along with a malware detection system utilizing an optimized LightGBM model. The models were trained using diverse datasets (ECU-IoHT, ToN-IoT, Edge_IIoTset, and EMBER) to ensure comprehensive coverage of potential attacks, and their performance was evaluated using standard metrics.

However, the article acknowledges several challenges, including the complexity of deploying such a sophisticated system across various healthcare network locations, the dependence of model effectiveness on the diversity and quality of training datasets, the need for continuous updates and retraining to adapt to evolving cyber threats, and the significant resource requirements in terms of computational power, time, and expertise. This highlights the intricate balance between advanced cybersecurity measures and practical implementation challenges in the healthcare sector.

The same researcher group otoum et al., [176] built upon their prior research [112] by incorporating a new dataset, the Edge-IIoTset dataset, and introducing an additional algorithm (CNN) alongside the Deep Neural Network (DNN). In this study, they proposed a Fault-Tolerant Learning (FTL)-based Intrusion Detection System (IDS) designed to enhance the security of healthcare-connected devices. The utilization of both DNN and Convolutional Neural Network (CNN) algorithms allows for the training and transfer of parameters from peripheral models, culminating in the creation of a comprehensive global model. Notably, this global model is tailored to address specific requirements without compromising user privacy.

A comprehensive study was put forward by Das et al., [177] to identify and address the complex challenges posed by cyberattacks on IoMT systems, which included device security vulnerabilities, data breaches, and potentially life-threatening impacts. A detailed examination of various cyberattacks such as DoS and DDoS attacks, MIMT attacks, password attacks, phishing, and malware attacks are involved along with their potential effects on patient safety, data privacy, and the integrity of healthcare systems. This study also involved a review of existing security measures, including protocols, cryptographic algorithms, and machine learning techniques, to understand the current state of cybersecurity in the IoMT landscape.

However, this research acknowledges several challenges and limitations, including the complexity and ever-evolving nature of cyber threats in IoMT. The difficulty of securing devices with limited computational resources, the integration of diverse and emerging technologies like blockchain and machine learning, and the critical need to balance data sharing with strong security and privacy measures are also discussed.

Aljuhani A., et al., [178] present an innovative approach to securing the Internet of Medical Things (IoMT), especially focusing on devices with limited resources. They propose a robust and efficient intrusion detection system that is not only capable of identifying threats but also explaining its decisions, thereby ensuring transparency and trustworthiness in its operations. To achieve this, the authors propose a Software as a Service (SaaS) model, utilizing Particle Swarm Optimization (PSO) for efficient feature engineering and an ensemble of machine learning and deep learning models for detection. The system employs SHapley Additive exPlanations (SHAP) for interpretability and is deployed on edge computing infrastructure to minimize resource usage on IoMT devices.

However, the work faces significant challenges, such as the complexity of deploying a SaaS solution in edge computing infrastructures, the constraints of optimizing performance in resource-limited settings, the dependence on effective initial feature engineering, the need for continuous updates to contest growing cyber threats, and the challenge of balancing explainability with system performance.

Nandy S. et al., [179] introduce a novel intrusion detection system that employs a Swarm-Neural Network (Swarm-NN) methodology, specifically tailored to address the security needs of resource-constrained IoMT devices. The core of this approach combines the principles of swarm intelligence with neural networks to efficiently detect cyber threats while accommodating the limited computational capabilities of IoMT devices. The system utilizes an Empirical Intelligent Agent (EIA) for processing health monitoring data at the network's edge and employs feature selection and optimization techniques to improve efficiency. This methodology is evaluated using the ToN-IoT dataset, which simulates various attack scenarios in IoMT settings, and the system's effectiveness is gauged using standard metrics like accuracy, precision, and recall. The complexity of integrating swarm intelligence with neural networks, the constraints of operating within limited resources, the dependence on high-quality training data, the need for continuous adaptation to evolving cyber threats, and balancing detection accuracy with resource efficiency are some of the challenges faced by researchers in this study.

Nayak et al., [180] proposed a framework to improve cybersecurity in the Internet of Medical Things (IoMT) through a novel approach combining Extreme Learning Machine (ELM) and Bayesian Optimization. This method is designed to efficiently detect cyber-attacks within IoMT by analyzing large volumes of data from various sensors and devices. They tackled addressing the security vulnerabilities and ensured data integrity and privacy within IoMT networks. Still, this research identifies several challenges and limitations in the field of the Internet of Medical Things (IoMT). First, ensuring interoperability and compatibility among diverse IoMT devices is a major challenge due to varying software versions, power consumption capabilities, protocols, and security standards, leading to potential security vulnerabilities and performance issues.

Additionally, the massive influx of data generated by these devices poses a significant challenge in terms of data overload, impacting the efficiency of data access and processing. The proliferation of IoMT devices also increases the attack surface, making the system more vulnerable to cyber threats. Another limitation is the obsolescence of existing software infrastructure in the healthcare sector, which hinders the integration of advanced IoMT solutions. Connectivity and bandwidth issues further complicate the effective deployment and operation of IoMT devices. Security remains a paramount concern, given the sensitive nature of healthcare data. Lastly, navigating and adhering to government regulations related to IoMT adds another layer of complexity along with the challenges in interpreting the diverse and complex data from various IoMT devices.

This study also proposes expanding its scope to enhance security and privacy measures specifically for cloud and fog-based dynamic environments within IoMT. Furthermore, it suggests exploring the potential of deep learning neural networks to learn features in IoMT environments that have not been previously trained, aiming to further strengthen the security framework in this rapidly evolving field.

Aljuhani [181] presents a novel framework combining intrusion detection systems and blockchain to enhance the security of IoMT networks. It employs fog computing to enable effective and efficient cyberattack detection close to the data source while using blockchain to maintain data integrity and privacy. Despite its innovative approach, the study acknowledges challenges such as scalability, computational resource constraints, and the complexity of implementation. The future work involves conducting more experimental validation using real-world IoMT data to further refine and test the effectiveness of the framework.

Swarna et al., [182] focus on developing an efficient Intrusion Detection System (IDS) for the Internet of Medical Things (IoMT). The primary objective is to secure IoMT architecture by accurately classifying and predicting cyberattacks using a deep neural network (DNN) model. This study is critical due to the growing reliance on IoMT and the need to protect medical data and devices from cyber threats. The methodology involves a unique blend of feature engineering using Hybrid Principal Component Analysis (PCA) and Grey Wolf Optimization (GWO) for optimal feature selection and dimensionality reduction. It also employs one-hot encoding and standard scaler normalization for data pre-processing, and the proposed DNN model is compared against other machine learning models to establish its efficacy.

Designing scalable IDS models that can adapt to the dynamic and unpredictable nature of cyberattacks is complex. Efficiently managing the vast amounts of data generated in IoMT and ensuring the optimization process doesn't omit critical information is challenging. The paper suggests future work could focus on enhancing the optimization techniques to better handle the complexity of IoMT data and continuously improving the DNN model for increased accuracy and efficiency. Additionally, applying and testing the system in real-world IoMT scenarios is proposed for practical validation and to address the evolving landscape of cyber threats in the IoMT environment.

Jagatheesaperumal et al., [183] focus on exploring the use of modern technologies like the Internet of Things (IoT), 5G networks, artificial intelligence (AI), and big data analytics in enhancing healthcare solutions. The motive behind this comprehensive survey is to systematically address and eliminate cyber threats in healthcare applications, thereby reducing human errors and enhancing the security and resilience of healthcare systems. The study presents a detailed taxonomy of existing technologies, examining their application areas, particularly in terms of security aspects, in the healthcare sector. An IoT-enabled smart pill bottle prototype is also designed and presented as a case study to provide a better understanding of how these technologies can be applied effectively in real-world scenarios.

This research discusses the potential of security-enhanced smart healthcare services powered by modern technologies, as recognized by the World Health Organization (WHO) considering increasing global health expenditure. These technologies have been instrumental in the early detection of various diseases, indicating the need for their widespread integration across healthcare operations. However, the study also identifies and summarizes state-of-the-art research challenges in healthcare, highlighting potential research gaps and future directions. It emphasizes the need for continued research to enhance the security aspects of modern healthcare systems, thereby addressing the prominent open-ended research challenges identified in the survey.

Wagan et al., [184] developed an innovative framework, named the Duo-Secure IoMT framework, which utilizes multi-modal sensory signals' data to differentiate between routine IoMT devices' data and attack patterns. This approach is particularly crucial in the context of prevalent cyber threats like botnet-based distributed denial of services (DDoS) and zero-day network attacks that disrupt regular IoMT operations. The proposed model combines dynamic Fuzzy C-Means clustering with a customized Bi-LSTM technique, aiming to securely process sensory medical data and identify attack patterns within the IoMT network. To evaluate the effectiveness of this framework, the study uses a heart disease dataset with 36 attributes and 18,940 instances, focusing on the dual objectives of predicting heart issues and identifying network malware. The performance evaluation reveals promising results, with the model achieving an individual accuracy of 92.95% and a multimodal joint accuracy of 89.67% in the IoMT-based distributed network environment.

This research didn't detail challenges and limitations, but they likely include issues related to the practical implementation of the framework in real-world IoMT settings. They also discuss the challenge of maintaining accuracy and reliability under diverse and evolving cyber threats, and

the potential resource intensity required for deploying and sustaining such an advanced multi-modal system. Additionally, scalability across different IoMT platforms and the generalizability of the results to other medical datasets may also present significant concerns.

A Zero-Knowledge Proofs (ZKP) based Authenticated Key Agreement (AKA) protocol for sustainable healthcare, particularly for Internet of Things (IoT) applications has been proposed by Gaba et al., [94]. By using ZKP and Physically Unclonable Function (PUF) for mutual authentication and key agreement in IoT networks, ensuring data integrity, confidentiality, and resistance to cyber threats with minimal computational, storage, and communication expenses. In this way, they enhance security in IoT-based healthcare systems, addressing vulnerabilities like unauthorized access and attacks on confidential medical information.

This research addresses limitations like resource constraints in IoT devices and challenges in securing IoT-enabled healthcare systems against various cyber-attacks. It includes a detailed security analysis, both formal and informal, proving the robustness of the proposed scheme against attacks like replay, impersonation, MITM, and physical tampering. For future work, authors are likely focused on further enhancing the protocol's efficiency, scalability, and robustness, possibly exploring its application in broader IoT contexts beyond healthcare.

Sills et al., [185] aims to address security vulnerabilities in medical IoT devices by creating a comprehensive repository of Cyber Threat Intelligence (CTI), enabling the use of AI-based cyber defence systems. For this purpose, they proposed a system that generates CTI from sources such as manufacturer alerts, and ICS-CERT, and augments it with data from Wikidata and FDA's AccessGUDID. The combined information forms a Cybersecurity Knowledge Graph (CKG) that is further enhanced through graph embeddings. The study evaluates the impact of knowledge augmentation on the quality of embeddings using the Mean Average Precision (MAP) metric.

They also discuss some challenges in terms of the lack of extensible big data resources for medical device vulnerabilities and the need for knowledge augmentation, and the complexity of connecting diverse data sources in the CKG is also a very important matter. Secondly, Security risks associated with medical IoT devices, such as data breaches and device compromise, highlight the urgency of creating a reliable knowledge base to enhance cybersecurity measures in healthcare settings.

The research proposed by Banyal et al., [49] primarily aims to explore and enhance the application of Computational Intelligence (CI) techniques in healthcare, with a special emphasis on bioinformatics and the Internet of Medical Things (IoMT). They investigate diverse applications of CI in healthcare, including diagnostics, predictive analytics, and personalized medicine. This research also covers several CI-based paradigms like artificial neural networks, fuzzy systems, and machine learning, highlighting their potential in medical and bioinformatics fields.

The researchers face challenges in terms of data labelling, security concerns, and the integration of CI in medical applications, emphasizing the need to overcome these hurdles to fully leverage CI's potential in healthcare. In this regard, this research likely discusses the potential expansion and further development of CI applications in healthcare as future work. This could include

more advanced AI models, better integration with emerging medical technologies, and strategies to overcome the discussed challenges, ultimately aiming to improve patient care and healthcare outcomes through computational intelligence.

2.5.6 Discussion

This scoping review summarizes various research articles from 2018-2023 focusing on enhancing cybersecurity in the healthcare sector, particularly on the Internet of Medical Things (IoMT). Prominent techniques used in these studies include ensemble learning, systematic literature reviews, structured literature reviews, machine learning, deep learning, federated learning and Blockchain.

Challenges and limitations identified by researchers encompass issues like dataset availability, computational resource limitations, system complexity, evolving cyber threats, data privacy, Heterogeneity and Interoperability in systems and implementation difficulties in diverse healthcare settings. Interestingly, in these recent studies, no one identified vulnerabilities by performing automated reasoning over existing knowledge. The visualization of these systems is not supported by knowledge graphs for IoMT or GenAI are used to augment or extend existing data with new information. Researchers usually use datasets for vulnerabilities or cyberattacks, but no one pulls through the vulnerabilities through API so new vulnerabilities can be detected as these are updated in the NVD dataset.

2.5.6.1 Key Findings

A comprehensive analysis of cybersecurity on the Internet of Medical Things (IoMT), elaborating on various methods and technologies discussed as under:

- *Ensemble Learning and Fog-Cloud Architecture:* This section explores a security framework combining ensemble learning with fog-cloud architecture, addressing challenges like cyberattack detection and system scalability in IoMT environments.
- *Machine Learning and Deep Learning Methods:* It examines the role of ML and DL in enhancing intrusion detection and prevention, emphasizing the evolving landscape of IoMT and related security concerns.
- *Federated Learning, AI, and Explainable AI:* The focus here is on using federated learning and AI to reinforce cybersecurity in healthcare systems, with a special emphasis on maintaining data privacy and improving operational efficiency.
- *Blockchain Technology:* This part explores how blockchain can be leveraged in IoT-based healthcare for heightened security and efficiency, while also discussing inherent challenges such as scalability and complex data handling.
- *Hybrid Models and Integrated Approaches:* It encompasses a variety of approaches like literature reviews and novel frameworks aimed at improving IoMT security, covering a wide range of aspects from intrusion detection to data privacy and efficient cyberattack classification.

2.5.6.2 Limitations

To strengthen the knowledge value of this scoping review, it is essential to acknowledge its limitations. Firstly, this review exclusively focused on studies written in English due to the researchers' proficiency in the English language, potentially overlooking valuable insights from non-English studies. Although the review searched five comprehensive databases, likely, certain journals publishing English-language studies on vulnerability and cyberattack detection on medical devices may not have been included in the search. Consequently, while the review's scope is extensive, it cannot be deemed fully comprehensive.

It is worth noting that the study of vulnerability and cyberattack detection on medical devices is still in its early stages. Nonetheless, despite the relative immaturity of this research area, the inclusion of a substantial number of studies leads the researchers to believe that the results offer a valid summary of the available evidence. This scoping review fosters a comprehensive understanding of the issues in question, ultimately leading to more effective approaches for addressing vulnerability and cyberattack detection in medical device challenges in remote patient monitoring with digital technologies.

2.5.7 Research Gaps and Priorities

This scoping review has highlighted key areas where current research is lacking, paving the way for future studies to address these gaps. It is important to acknowledge that the scoping review made no direct mention of the two underlying themes within this research, namely the value of Knowledge Organization Systems and Reasoning, since these two thematic areas are key components in the emerging research interest which inform some of the key novelty sections within this overall study. In simple terms, the scoping review was primarily evolved through two predominant search criteria (being Medical IoTs and Security of IoTs). Thus, when this discussion considers the important gaps that emerge because of the scoping review, these two areas require attention even though they are unsupported as jointly intersected elements by the literature that has been captured within the scoping review.

There are several possible reasons as to why these gaps appear in this part of the study. Firstly, the search terms used will specifically focus on reasoning and highlight the areas of overlap between medical IoTs and the security of IoTs. However, in isolation, part of the reasoning discourse may appear in Medial IoTs, whilst in other areas the same thematic elements may emerge separately in research based on the security of IoTs. Secondly, the emergence of Knowledge Organization Systems (whilst strongly embedded with many aspects of medical data including medical IoTs) remains as system-based information that is less likely to emerge within the security aspects of the scoping review. In combination (and based on these key factors) it has emerged as key findings of the scoping review that several thematic gaps exist, and these are therefore discussed below.

a. **Heterogeneity and Interoperability in systems**

   A Knowledge Organization System (KOS) is a structured framework crucial for organizing and categorizing data and streamlining information management. It offers substantial benefits, including enhanced efficiency and accuracy in information retrieval, facilitating knowledge sharing across various organizational units, and improving large data volume management.

KOS aids in understanding complex information structures, fostering learning and knowledge discovery. It supports heterogeneity through standardized structures for interoperability and flexible classification schemes. These systems are adept at handling a wide range of subjects and establishing semantic relationships among diverse data sets. The customization capabilities of KOS ensure they meet the specific needs of different domains, thereby enhancing the organization of heterogeneous information. Examples of KOS include Taxonomies, Thesauri, Ontologies, and Classification Schemes.

b. **Reasoning Capability**

Reasoning refers to the use of computer systems to simulate human reasoning, particularly in identifying vulnerabilities. One example is automated reasoning, which is primarily concerned with developing computing systems capable of automating the process of making inferences. This field intersects with artificial intelligence, theoretical computer science, and philosophy. The ultimate goal of automated reasoning is to create computer programs capable of reasoning either completely or nearly automatically, using logic-based approaches. Reviews indicate a scarcity of research on applying automated reasoning to detect security vulnerabilities in IoMT (Internet of Medical Things) systems. This gap suggests a potential area for future research, where automated systems could analyze existing knowledge and data to identify and mitigate vulnerabilities in IoMT systems.

c. **Data Visualization and Knowledge Representation**

As data becomes an increasingly important part of decision-making, the role of data visualization in interpreting this data grows more significant. The key is to choose the right kind of visualization that complements the data and makes it easy to understand and interact with. With the increasing amount of data, knowledge graphs have become crucial in making data 'smart.' A Knowledge Graph (KG) is an advanced and structured form of knowledge representation that uses a graph-structured data model to store and interrelate information about entities and their relationships. These entities can be objects, events, situations, or concepts from the real world or abstract domains. By allowing flexible data schemas and representing complex real-world relationships, they surpass the limitations of traditional data repositories. The use of globally unique identifiers in knowledge graphs also facilitates data integration and publishing. This scoping review notes a lack of visualizations specifically tailored for IoMT (Internet of Medical Things) systems. These graphs could be instrumental in understanding complex relationships and interactions within IoMT ecosystems, thus aiding in better management and security of these systems.

d. **Evolving cyberthreats related to IoMT devices**

This literature review highlights the significant security challenges faced by the healthcare sector. It points out that the rise of cyber threats poses risks not only to the industry but also impacts individuals and the technologies used in smart home healthcare applications. These studies focus on vulnerabilities identified through historical datasets or past cyberattacks. However,

there's a gap in research focusing on the real-time detection of vulnerabilities, particularly using APIs (Application Programming Interfaces) to identify new threats as they emerge, such as those updated in the National Vulnerability Database (NVD). This area is crucial for timely and effective responses to emerging cyber threats in IoMT systems.

e. **Lack of Dataset availability**

There are no publicly available datasets specifically addressing vulnerabilities or cyberattacks on medical devices for remote patient monitoring. Some researchers have utilized datasets like ECU-IoHT and IIoT sensors, including ToN-IoT, which are available online but do not directly support IoMT settings. Instead, researchers often rely on simulations or case studies to evaluate the performance of their systems in this context.

2.5.8 Conclusion for Scoping Review

The Internet of Medical Things (IoMT) has significantly contributed to connecting patients with healthcare providers, but it also brings cybersecurity challenges. Vulnerabilities in IoT smart homes have resulted in cyberattacks, highlighting the need for robust security measures.

This study involves a comprehensive scoping review and the identification of research issues using various search engines, such as Web of Science and Google Scholar, and databases available through the ECU library, including the IEEE Digital Library, SpringerLink, and ACM Digital Library. The primary focus was on sourcing research articles related to the Internet of Medical Things (IoMT), knowledge organization systems, and the vulnerabilities and cyberattacks affecting IoT networks used in remote patient monitoring. The literature review primarily analyzed existing architectures and systems developed by various researchers. Additionally, it identifies research gaps in areas such as heterogeneity and interoperability, evolving cyber threats, dataset availability, reasoning capability, and data visualization. It was observed that there is a limited amount of literature specifically addressing vulnerabilities in IoMT devices employed in remote patient monitoring settings. Furthermore, this review lays the groundwork for future research aimed at enhancing IoMT security and efficiency.

2.6 Summary of Chapter

This chapter provides a comprehensive review of information and research. It covers the broad areas of IoMT and cybersecurity, with a specific focus on remote patient monitoring, vulnerabilities and cyberattacks in the field of IoMT and healthcare. Existing models and frameworks in this domain are also discussed. Additionally, the tools and technologies that will be used to develop the semantic framework are covered.

Furthermore, the scoping literature review within this chapter contributes to the foundational structure and research depth of this thesis by providing clear insights into research gaps and areas where future and emerging research will unfold. This chapter presents a clear narrative for addressing key issues and reinforcing the known and unknown elements of this doctoral research study.

Chapter 3

Research Methodology and Design

This chapter outlines the research approach implemented to devise a solution to the problem, ensuring that the methodology is grounded in reputable research methods to enhance its scientific credibility within the research community focused on IoMT and cybersecurity. It describes the workflow and the different research stages involved in establishing a semantic framework to achieve the desired outcomes.

This chapter discusses the research methodology used in this research and the research design proposed to achieve the research objectives. The main part of the research design is the development of a semantic framework proposed to detect vulnerabilities in the IoMT environment, particularly in remote patient monitoring.

3.1 Research Methodology and Design

Research methodology is a systematic process designed to address and solve research problems by employing validated research methods. A research method may refer to a procedure, tool, algorithm, or component critical to the investigative process. The methods utilized in this research have been carefully planned and scientifically validated to include statistical studies, experimental procedures, theoretical approaches, measurements, observations, hypotheses, and more. These methods facilitate the collection of data and samples, enabling the discovery of solutions to specific problems [186].

In the field of computer science, researchers employ various methods to conduct their experiments. Broadly, these methods fall into two main categories: the scientific method and the mathematical method [187], [188]. The scientific method, often regarded as the optimal paradigm for understanding software processes, products, people, and environments, involves observing the world, proposing models, measuring, analyzing, and validating these models. It is subdivided into two approaches: the empirical method and the engineering method. This research adopts the scientific approach, specifically focusing on the engineering method subcategory. Research grounded in science and engineering enables researchers to validate theoretical predictions [188]. In this regard, researchers often propose solutions to problems by developing, measuring, and analyzing techniques, methodologies, models, algorithms, or frameworks against existing solution. In the engineering domain, the fundamental goal of 'creating functional solutions' is realized through three distinct levels, as identified by: the

conceptual level, the perceptual level, and the practical level [189]. Each of these levels is further elaborated as:

Conceptual Level: At this initial stage, innovative ideas are formulated, leading to the creation of new concepts. This process involves a detailed analysis of the problem at hand.

Perceptual Level: This level involves the development of new techniques based on novel approaches. It encompasses the design and development of specific tools, environments, or appropriate systems through implementation.

Practical Level: At this final stage, the focus shifts to the application of testing and validation techniques. Experimentation is conducted based on real-world scenarios, employing either laboratory or testing methods are used.

This thesis focuses on developing a semantic framework designed to facilitate partial automation and enhance the security posture of IoT networks used in remote patient monitoring systems. At the core of this framework is a domain ontology that encapsulates the semantics of the concepts and properties critical to the main security aspects of IoT medical devices utilized in such systems. This ontology is augmented with a comprehensive ruleset, complex queries, and mechanisms that enable automated reasoning over aggregated knowledge. Consequently, to address the various tasks required to develop a solution, the science and engineering research methodology has been adopted as the primary research method for this thesis. Figure 3.1 shows the research pipeline based on the Science and Engineering research methodology for this thesis work.

3.2 Research Phases

This research is structured into two main phases, employing scientific and engineering methodologies. The first phase, problem formulation, clearly outlines the definition and origin of the problem. The second phase, proposing a solution, describes in detail the workflow of activities designed to resolve the problem.

3.2.1 Problem Formalization

The research began with the identification of research problems, followed by a literature review to explore the different techniques employed to tackle these issues. Based on the existing literature concerning modelling, processing and visualization challenges and verification and validation of IoMT security, the problem is formalized and presented in an algorithmic manner. This algorithm is designed to validate a use case and systematically detect vulnerabilities in Medical IoT Devices, identify potential attacks that could exploit these vulnerabilities, assess any possible adverse side effects from such attacks, and finally, determine appropriate countermeasures to protect against these vulnerabilities.

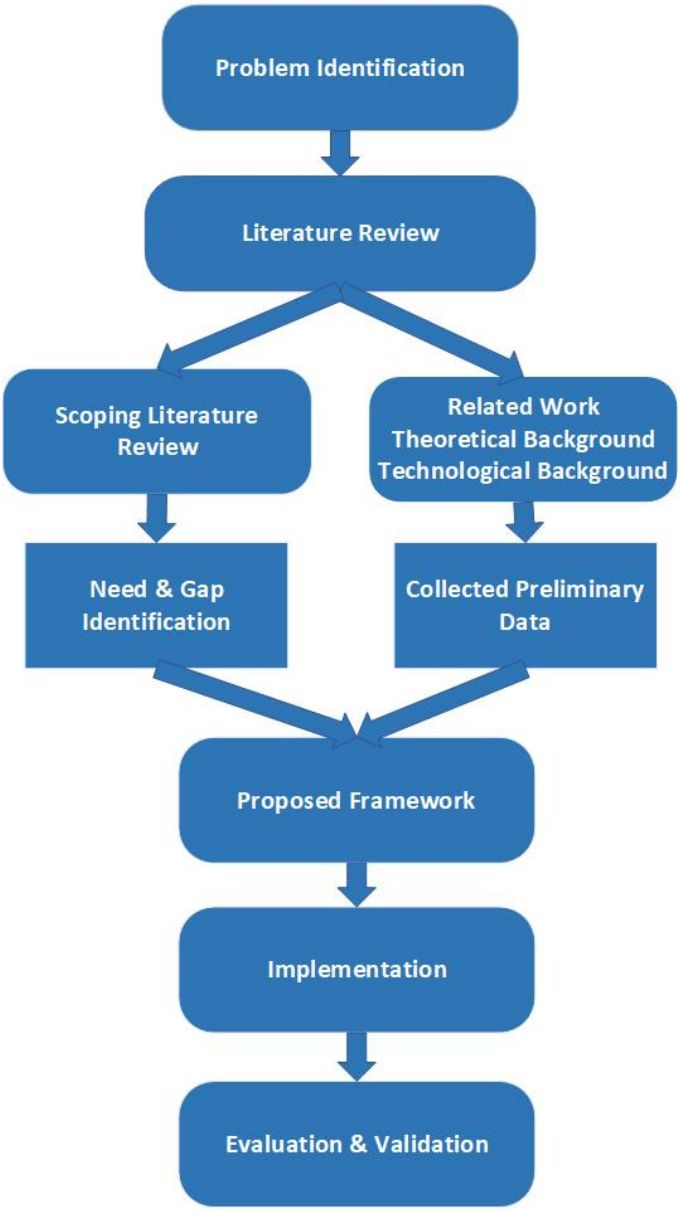

Figure 3.1: The Science and Engineering Methodology for Semantic Framework Development.

Use Case: If a patient is using a medical device, such as a defibrillator or a blood pressure monitor, that connects to services through network technologies like Wi-Fi or cloud-based systems, there is an inherent risk of vulnerability. These vulnerabilities could potentially be exploited by cyber attackers to compromise device functionality or patient data privacy. This not only jeopardizes patient health but also undermines trust in healthcare technologies. To safeguard both the patient and the device from adverse outcomes, it is crucial to implement robust countermeasures that effectively mitigate these vulnerabilities.

3.2.2 Research Phase 2: Proposed Solution

In this thesis, the primary aim is to develop a semantic framework to enhance the security posture of IoT networks used in remote patient monitoring (RPM) through partial automation and visualized data in a knowledge graph. This framework will query existing knowledge to analyze insights and identify

Algorithm 1 Vulnerability Detection in Medical IoT Devices

Require: Person P, Medical Device MD, Service S
Ensure: Detected Vulnerabilities V, Potential Attacks A, Adverse Side Effects ASE, Countermeasures C
0: $V \leftarrow \emptyset$ **Vulnerability** in MD **do**
0: **if Vulnerability** is found **then then**
0: Add Vulnerability to V
0: **end if**
0: Identify potential attacks exploiting the vulnerabilities: **Vulnerability** in V **do**
0: $A \leftarrow IdentifyPotentialAttacks(Vulnerability)$ **Attack** in A **do**
0: $ASE \leftarrow AssessAdverseSideEffects(Attack)$
0: Select countermeasures to mitigate the vulnerabilities and protect the medical device: **Vulnerability** in V **do**
0: $C \leftarrow SelectCountermeasures(Vulnerability)$
0: **return** V, A, ASE, C =0

new vulnerabilities, providing information about their severity and impact while suggesting mitigation strategies.

In detail, at the core of this framework is a domain ontology that encapsulates the semantics of concepts and properties essential to the primary security aspects of IoT devices in such environments. The framework will be supplemented with a comprehensive set of rules and mechanisms that enable automated reasoning over aggregated knowledge. Additionally, the aggregated knowledge will be stored and visualized in a knowledge graph, with queries performed to extract meaningful information regarding vulnerabilities, their impact, and severity. Table 1 provides a concise overview of the phases included in the solution methodology.

Table 3.1: Solution Methodology Phases

Solution Methodology Phases		
Phase	**Title**	**Description**
Phase I	Conceptual Model	To define key concepts, relationships, individuals, and axioms for the conceptual model
Phase II	Prototype Development	Use the semantic web technologies (OWL, RDF, and XML), de-facto standards to verify the conceptual model by developing a prototype
Phase III	Semantic Framework	To implement the semantic model and store CTI information in a knowledge graph
Phase IV	Evaluation and Validation	Evaluation and validation based on use cases and existing framework

The solution methodology starts with developing the conceptual model for ontology development, followed by prototype development. After successfully developing the prototype, the process continues

with the implementation of the semantic framework, where the aim of this research is achieved. Finally, the semantic framework is validated against existing frameworks in the same domain of research. These four phases are illustrated in Figure 3.2, which shows the flow of the solution methodology.

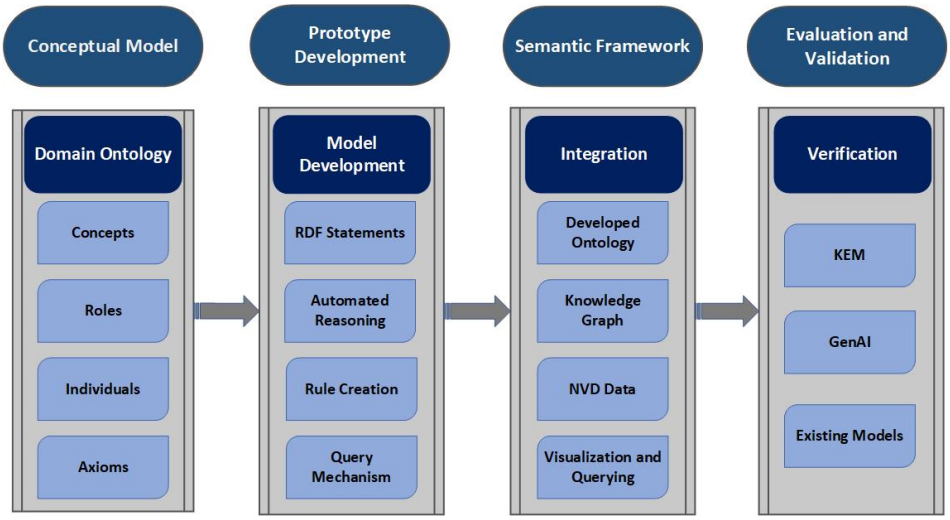

Figure 3.2: Pipeline of activities for the proposed Solution.

3.2.2.1 Phase I- Conceptual Model

In the field of software engineering, conceptualization plays a crucial role. This involves defining principles and design criteria essential for developing the domain ontology. Conceptualization organizes domain knowledge (background knowledge) into a conceptual model that articulates the problem and its solution using domain-specific vocabulary. Such structuring of information simplifies the understanding and communication of complex concepts within the domain.

This model establishes connections between concepts through various properties (relationships) that serve diverse purposes within the Internet of Medical Things (IoMT) context, addressing different scenarios and use cases. It offers a centralized repository and tools that enable effective sharing and communication among all system participants. This not only accelerates the development process but also enhances interoperability and the correlation of test results. Details about the conceptual model are provided in **Chapter 4**. In subsequent phases, this conceptual model is implemented in RDF, visualized, and queried within a knowledge graph that stores Cyberthreat Intelligence (CTI) for semantic representation and data integration.

3.2.2.2 Phase II- Prototype Development

In this phase, a prototype is developed to demonstrate the detailed workings of the proposed conceptual model. It is specifically designed to model and reason about anomalies and vulnerabilities within the IoMT system. The well-defined formalism RDF is utilized to create a domain ontology, capturing the semantics of the domain in terms of concepts and relationships. This includes defining instances of medical devices, vulnerabilities, and IoT networks.

Semantic annotation is performed to enrich the domain ontology within the defined setting. Additionally, rule-based reasoning is applied atop the semantic modeling to infer hidden facts from the

knowledge base. Moreover, the effectiveness of this prototype is validated through use cases derived from hypothetical scenarios. The prototype development is presented in **Chapter 5**.

3.2.2.3 Semantic Framework

This phase is crucial for achieving the primary objective of this research. The proposed semantic framework aims to detect vulnerabilities and anomalies in the system. It creates a semantic model and performs reasoning over aggregated knowledge using a predefined ruleset. Furthermore, it integrates the semantic model with a knowledge graph enriched with medical device data and incorporates National Vulnerability Database (NVD) CVE information via an API[1]. This methodology empowers the framework to predict new vulnerabilities and update the system, thereby enhancing the security of remote patient monitoring systems. Finally, a query mechanism is used to access vulnerabilities related to medical devices, assess their impact, and determine their severity. The Semantic Framework is presented in **Chapter 6 and Chapter 7**.

3.2.2.4 Evaluation and Validation

Evaluation and validation are critical elements in scientific and engineering methodologies, essential for ensuring the reliability, accuracy, and applicability of research findings and technological innovations. The evaluation assesses the performance and effectiveness of a model against specific objectives, while validation confirms the accuracy of these results, ensuring they meet the required specifications, standards, or user expectations.

In this study, evaluation is performed at various phases. The evaluation of the conceptual model has been done in **(Chapter 4)**. The prototype for ontology development is also evaluated in **(Chapter 5)**, while the evaluation of the whole MIoT semantic model is presented in **(Chapter 7)** by using knowledge engineering methodologies and generative AI techniques applied to use cases from a laboratory case study. These methodologies and techniques are employed to evaluate the outcomes of reasoning processes and to assess the performance of rule set generation. Additionally, the MIoT semantic framework is validated **(Chapter 7)** against existing framework in the research field to determine its accuracy and adequacy in addressing the research problem. It also shows how the MIoT Semantic Framework is more robust and efficient as compared with existing models.

3.3 Summary of the Chapter

This chapter outlines the detailed research methodology and design proposed to address the research problem and achieve the objectives of this thesis. It details a structured pipeline of activities, systematically organized to ensure the successful achievement of the desired outcomes. By specifying each step of the research process, this chapter provides a clear roadmap for the study, facilitating a thorough and logical approach to solving the identified challenges.

[1]Application Programming Interface

Chapter 4

Developing a Novel Ontology for Cybersecurity in Internet of Medical Things-Enabled Remote Patient Monitoring

This chapter discusses the development of an ontology for cybersecurity in the Internet of Medical Things (IoMT). In this regard, a MIoT conceptual model is proposed that includes concepts, roles, and individuals related to IoMT and cybersecurity by applying ontology engineering methodology. This chapter has been published as a journal article in *Sensors* [13], and it is available online at `https://doi.org/10.3390/s24092804`.

Abstract

IoT has seen remarkable growth, particularly in healthcare, leading to the rise of IoMT. IoMT integrates medical devices for real-time data analysis and transmission but faces challenges in data security and interoperability. This research identifies a significant gap in the existing literature regarding a comprehensive ontology for vulnerabilities in medical IoT devices. This chapter proposes a fundamental domain ontology named MIoT (Medical Internet of Things) ontology, focusing on cybersecurity in IoMT (Internet of Medical Things), particularly in remote patient monitoring settings. This research will refer to similar-looking acronyms, IoMT and MIoT ontology. It is important to distinguish between the two. IoMT is a collection of various medical devices and their applications within the research domain. On the other hand, MIoT ontology refers to the proposed ontology that defines various concepts, roles, and individuals. MIoT ontology utilizes the knowledge engineering methodology outlined in Ontology Development 101, along with the structured life cycle, and establishes semantic interoperability among medical devices to secure IoMT assets from vulnerabilities and cyberattacks. By defining key concepts and relationships, it becomes easier to understand and analyze the complex network of information within the IoMT. The MIoT ontology captures essential key terms and security-related entities for future extensions. A conceptual model is derived from the MIoT ontology and validated through a case study. Furthermore, this paper outlines a roadmap for future research, highlighting potential impacts on security automation in healthcare applications.

4.1 Introduction

In the era of Industry 4.0, the Internet of Things (IoT) has rapidly expanded, particularly in the healthcare sector, where the Internet of Medical Things (IoMT) has emerged as a specialized branch. IoMT focuses on integrating interconnected medical devices and information systems, revolutionizing healthcare by enabling real-time data collection, analysis, and transmission [190]. This technology offers opportunities for remote patient monitoring, improved medical processes, and improved decision-making.

IoMT operates through a network of connected medical devices, sensors, and information systems, facilitating the collection and transmission of continuous automatic and health data. Various devices, such as vital signs monitors, medication delivery tools, fitness trackers, and home monitoring devices, contribute to this interconnected system. Data collected can be transmitted to healthcare professionals, hospitals, or cloud-based systems for analysis and storage, leading to innovative medical applications such as the remote monitoring of chronic patients and personalized healthcare, eventually advancing diagnosis and treatment in the healthcare industry [191], [192].

Despite the advances and expansion of Internet of Medical Things (IoMT) technology, numerous challenges must be faced to ensure its widespread success and adoption. These challenges encompass issues such as data security and privacy, ensuring the interoperability of devices and systems, efficient data management, and addressing the long-term sustainability of technology. Knowledge organization systems (KOSs) are one of the solutions used to organize and categorize information, knowledge, and data, making it more accessible, searchable, and understandable in the field of IoMT. These systems help individuals and organizations efficiently manage and retrieve information. Various types of knowledge organization systems exist, including taxonomies, thesauri, ontologies, and controlled vocabularies, among others [135]. The choice of a particular KOS depends on the nature and requirements of the information and the users. For example, a taxonomy might be sufficient for simple categorization tasks, while an ontology would be better suited for complex data analysis and Semantic Web applications.

4.1.1 The Need for a Cybersecurity Ontology for Remote Patient Monitoring

In the dynamic field of healthcare technology, especially in remote patient monitoring (RPM), the importance of robust cybersecurity measures has grown significantly. With medical devices becoming increasingly interconnected and reliant on networked systems, the threat of cybersecurity risks such as data breaches and device vulnerabilities has become more pronounced [41]. In this situation, maintaining cyber-resilience across networks poses significant challenges, particularly concerning data security, scalability, heterogeneity, interoperability, and integration. These difficulties arise from the exposure of data and the diverse functionalities and specifications of various devices within the network [39]. Hence, there is a crucial need for methods and tools to promptly detect data breaches and respond effectively to identified cyberattacks. In this regard, ontology is a formal representation of knowledge or concepts within a specific domain [193].

The primary benefit of ontologies lies in interoperability. By establishing a shared vocabulary,

data can be shared and exposed using a formal definition, enabling others to understand and utilize it effectively. This facilitates the development of applications that consume the data with interoperability and RDF (resource description framework), forming the foundation of the Semantic Web concept. Secondly, ontologies support inferencing, where fragments of knowledge within the ontology can be used to obtain new perceptions/knowledge. This process involves inferring new knowledge based on existing data, allowing for the derivation of additional facts from existing data by using ontological principles [194].

This paper proposes a fundamental domain ontology named MIoT ontology, focusing on cybersecurity in IoMT, especially in remote patient monitoring settings. This research will refer to two closely related acronyms that may appear similar. It is important to distinguish between the two terms used in this research: IoMT (Internet of Medical Things) and MIoT (Medical Internet of Things) ontology. IoMT refers to the network of interconnected medical devices and applications that collect and transmit health data over the Internet for monitoring, diagnosis, and treatment purposes. On the other hand, MIoT ontology specifically relates to the structured representation and organization of knowledge within the domain of medical IoT, focusing on the semantics and relationships of medical devices and vulnerabilities. The development of an MIoT ontology would provide a structured framework for organizing and categorizing cybersecurity-related concepts such as vulnerability, exploit, and attack, defining their relationship within the RPM ecosystem. By clearly defining the key concepts and their connections, this ontology would empower healthcare providers and cybersecurity professionals to better comprehend, evaluate, and mitigate potential vulnerabilities to patient data and device security.

4.1.2 The Role of Semantic Models in the Internet of Medical Things

A semantic model is a high-level, abstract representation of data that focuses on capturing and conveying meaning rather than just structure or syntax, allowing interpretation from instances. In data integration and exchange scenarios, semantic models ensure effective understanding and integration of data from different sources, such as medical sensors. By encoding meaning and relationships between data elements, semantic models enable interoperability between systems, providing a structured framework for organizing meaningful relationships, as demonstrated by RDF triples in Semantic Web data.

The Semantic Web, an extension of the World Wide Web (W3C) [16], aims to make web content more machine-understandable using standard semantic technologies. Its success relies on the quality of its underlying ontologies, which provide a shared understanding of a domain for communication between people and heterogeneous systems. Ontologies facilitate interoperability by establishing a common understanding of concepts and relationships, crucial for data integration and semantic interoperability. They also aid in retrieving heterogeneous information from cross-domain applications. Semantic web technologies, including RDF, OWL, and XML, are utilized to construct ontologies for different domains [104].

Our research paper aims to develop a fundamental ontology for the IoMT domain; we named it the MIOT (Medical Internet of Things) ontology, focusing on essential terms related to the cybersecurity domain. To achieve this, we employ scientific methods and tools in the definition process and subsequently demonstrate the ontology's applicability to information systems. The resulting ontology serves

as a conceptual ontological model that assesses the potential for establishing semantic interoperability among medical devices from heterogeneous sources.

This paper is organized as follows: the existing work is discussed in Section 4.2. The ontological technology is introduced in Section 4.3, followed by a methodology of our research approach in Section 4.4. This methodology outlines the ontology's domain and relevant terminology, explores possible interfaces with existing ontologies, and defines important terms. It further shows the hierarchical structure for concepts derived from identified terms, specifying their required properties, followed by formal grounding with description logic. Subsequently, in Section 4.5, a conceptual model is derived from the ontology and validated through a case study. Finally, Section 4.6 is presented to discuss challenges and provide potential avenues for future research, followed by Section 4.7, where we summarize our work.

4.2 Related Work

This work seeks to enhance cyber-resilience in healthcare, where challenges such as interoperability, heterogeneity, scalability, integration, and visualization are dominant. Various standards and frameworks, including SNOMED CT [195], HIPPA [21], HL7 FHIR [20], STIX [196], NIST [196], [197], and HITRUST [198], among others, have been developed to address these concerns. For instance, the industry standard National Institute of Standards and Technology (NIST) revised its cybersecurity recommendations for healthcare in mid-2022, aiming to safeguard patients' health data to uphold the confidentiality, integrity, and availability of health data [34].

At the same time, researchers have responded to these challenges by leveraging semantic models and frameworks. For instance, the researchers in [199] conducted a comprehensive analysis of various technologies, system architectures, optimization factors, and challenges associated with implementing IoT in hospital settings. It serves as a link between business applications and sensors within a unified network, paving the way for the development of an interoperable smart hospital design. However, the research does not address the privacy and security risks associated with the creation of such a hospital design.

Gorrepati et al. [137] proposed an ontology-based modeling framework and IoT-based semantic M2M platform. The framework employs IoT healthcare domain ontologies to design knowledge frameworks, automate sequencing, and provide semantic descriptions of concepts and relationships. The use of SWRL rules helps overcome expressivity limitations in property association, enabling spatial connection reasoning. The constructed system, developed using Protégé and its plug-ins, focuses on enhancing hospital device interoperability and semantic annotation in IoT applications. Sharma et al. [63] proposed an IoT-powered, ontology-based remote access model and bio-wearable sensor system for the early detection of COVID-19, utilizing 1D biomedical signals, which contain PPG (photoplethysmography), ECG (electrocardiogram), accelerometer, and temperature. This ontology-based monitoring system analyzes the challenges around privacy and security issues and is also simulated by using a Cooja simulator to observe the efficiency of the proposed model.

A study proposed by Pazienza et al. [80], named the Digital Future project, where Semantic Web

services are combined with service-oriented architecture (SOA)-based principles using an IoE (Internet of Everything) platform to address interoperability at the semantic level, employing middleware components. In a parallel effort, Kotha et al. [109] focused on enhancing interoperability in healthcare IoT devices through a study leveraging natural language processing (NLP) techniques, including bidirectional encoder representations from transformers (BERT) for string matching and a fuzzy inference system (FIS) for data correlation. Although the study primarily aimed to improve data communication efficiency among healthcare IoT devices and demonstrated results to enhance IoT interoperability in healthcare, it did not directly address cyberattack detection.

A comprehensive scoping review was conducted by Luschi et al. [8] to identify and analyze available ontologies capable of representing all relevant use cases describing the hospital environment in relation to the European project ODIN and its future expansion. The review was conducted on the Scopus database in January 2023 using the PRISMA extensions for scoping reviews. Two reviewers screened 3225 documents that resulted from the database search. Finally, they filtered the results to a final set of 32 articles for the analysis of the results. In this scoping review, famous ontologies in the field of healthcare were discussed, such as the SNOMED-CT ontology (SCTO) [200], Dietary Lifestyle Ontology (DILON) [201], and International Classification of Diseases (ICD) [202], among others. However, the researchers solely concentrated on medical-related aspects and neglected security concerns.

In terms of ontology development for cybersecurity, a well-known ontology named the IDS (intrusion detection system) ontology was created by Undercoffer et al. [203]. IDS was extended as the Unified Cybersecurity Ontology (UCO) by Syed et al. [204] to establish a standardized framework for describing the cybersecurity domain. This initiative seeks to transition cybersecurity standards from mere syntactic representations to more semantically enriched ones. Specifically, the UCO serves as a semantic counterpart to STIX (Structured Threat Information eXpression) [196], incorporating references to external standards such as CVEs (common vulnerabilities and exposures), CWE (common weakness enumeration), and CAPEC (common attack pattern enumeration and classification), among others. UCO provides an overview of general cybersecurity concepts such as potential attacks, attack patterns, methods, etc., but dedicates minimal attention to describing the infrastructure itself.

Following this, Bruno et al. [205] introduced novel concepts such as asset and security mechanisms in the IoTSec ontology, which were not part of UCO [204], thereby providing a detailed overview of the infrastructure. The project's primary objective was to ensure that companies operating in the Internet of Things sector utilized their devices securely, aiding in the identification of vulnerabilities and critical points. However, a drawback of IoTSec lies in the static nature of its knowledge regarding vulnerability and threat classes. These aspects lack integration with external sources and require direct management and maintenance during ontology implementation. However, these ontologies are IoT-specific, but our work focuses on cybersecurity aspects for IoMT, particularly in a remote patient monitoring setting, where the MIoT ontology captures the semantics related to concepts and relationships for vulnerability detection in medical devices.

The existing literature in the fields of healthcare and cybersecurity highlights a substantial research gap, specifically the absence of a comprehensive ontology that can effectively offer knowledge

regarding vulnerabilities in Medical Internet of Things (IoT) devices [8; 202; 204]. In response, this research endeavors to introduce a novel MIoT ontology that not only addresses this gap but also provides a detailed mechanism for developing practical solutions by incorporating semantics.

4.3 Ontological Technology

Ontology was originally rooted in philosophy, denoting an explanation or description of objective existence, emphasizing the philosophical exploration of being and various types of existence. The term 'ontology' or (ontologia) was coined in 1613 independently by two philosophers, Rudolf Gockel and Jacob Lorhard [193]. In the realm of artificial intelligence (AI), Neches et al. [206] introduced the first AI-specific definition, characterizing ontology as the framework defining fundamental terms and relations that constitute the vocabulary of a particular domain, along with rules governing their combination to extend the vocabulary. Gruber T. [193] offered a widely adopted definition, presenting ontology as an explicit 'Specification of a Conceptualization'.

Pinto and Martins [207] defined ontology as ontologies fostering interoperability among information systems, enabling intelligent processing by agents, and facilitating the sharing and reuse of knowledge across various systems. They establish a shared and unified understanding of a domain, facilitating communication among individuals and heterogeneous and diverse application systems. Generally, ontologies consist of a collection of terms representing concepts organized in a hierarchical structure, along with specifications defining their meanings.

Over time, this understanding gained acceptance among scholars and engineers. In the field of artificial intelligence, the term 'ontology' is defined in various ways by different scholars. For this guide, ontology is a knowledge representation (KR) system based on description logics (DLs). Ontology is understood as a formal and explicit representation of concepts within a specific domain. Formal indicates that the ontology is machine-readable, while explicit refers to the constraints applied to concepts [208]. 'Classes' are referred to as 'concepts'). It includes the properties (or 'slots', also known as 'roles' or 'properties') that characterize each concept and the constraints on these properties (termed 'facets', also known as 'role restrictions'). Table 4.1 shows the difference between first-order logic (FOL), description logic (DL), and Web Ontology Language (OWL) terminology for concept, role, and constant [209].

Table 4.1: FOL, DL and OWL Terminologies

FOL, DL and OWL Terminologies		
FOL	**DL**	**OWL**
unary predicate	concept	class
binary predicate	role	property
constant	individual	individual

Numerous ontologies, such as description logic (DL) knowledge bases, have been created to offer comprehensive insights into diverse domains. An ontology comprises an ABox, containing assertion axioms between entities or between a concept and an entity, and a TBox, containing terminology axioms between two concepts [210; 211]. An ontology, when combined with specific instances (ABox, i.e., the instances of the model) of these classes (TBox model, i.e., the terminological component), forms what is known as a 'knowledge base' [212] and is usually represented in RDF and OWL. The definitions of these terms are given in Table 4.2. In the DL Knowledge base (KB), TBox is a set of 'terminological' axioms and Abox is a set of 'assertional' axioms [213].

In this regard, ontologies provide a conceptual framework for organizing knowledge. They define concepts or entities relevant to a specific domain or problem. Ontologies often have a hierarchical structure with broader, more general concepts at the top and narrower, more specific concepts below. This hierarchy allows for the classification and categorization of information.

Ontologies distinguish between classes (abstract concepts or categories) and instances (individual entities belonging to a class). For example, 'MedicalDevice' is a class, while 'BPMonitor' is an instance of the 'MedicalDevice' class. Ontologies specify properties or attributes associated with concepts. These properties describe the characteristics or features of instances. For example, a 'Vulnerability' class might have properties like 'hasCVEID' and 'publishedDate'. Ontologies also define relationships between concepts called object properties. These relationships provide context and meaning to the concepts and can be hierarchical *(is-a)*, part-whole *(has-part)*, spatial *(located-in)*, and temporal *(preceded-by)*.

Table 4.2: Abbreviations and Descriptions

Abbreviations and Descriptions		
Abbreviations	**Stands for**	**Description**
ABox	Assertional Box	A component that holds statements about individuals, such as OWL facts including type declarations, property-value relationships, as well as assertions of equality or inequality.
TBox	Terminological Box	A component that stores statements about classes, including OWL axioms like subclass relationships, equivalent classes, or disjointedness declarations.
KB	Knowledge Base	A combination of an ABox and a TBox represents an ontology.

In the context of vulnerability detection in IoMT, the domain MIoT ontology provides a structured and organized framework for categorizing, classifying, and searching for information related to vulnerabilities and cyberattacks in IoMT. This structured approach, along with semantics, improves

the efficiency and accuracy of vulnerability detection processes and enables better decision making in addressing cybersecurity attacks. For instance, ontology is used to model the relationships between various elements in the cybersecurity domain and remote patient monitoring, including medical devices, targets, vulnerabilities, exploits, and attacks.

4.4 A Proposed Methodology for Ontology Development

Developing an ontology is a collaborative task where domain experts can identify the concepts and define relationships in the domain work with knowledge engineers. Domain ontology is a very important part of our research work where we apply ontology engineering practices to develop the proposed ontology. However, note that there is not any particular or correct way to develop the ontology, and researchers apply different ways to develop the ontology [129; 214; 215; 216]. We utilize the knowledge engineering methodology (KEM) outlined in Ontology Development 101 [212], along with the structured life cycle proposed by Gómez-Pérez et al. [217]. These methodologies were chosen for their comprehensive step-by-step procedures in ontology development.

Ontology Development 101 adopts a process-oriented approach, accommodating setbacks and emphasizing continuous improvement through multiple iterations. This methodology is particularly crucial for our ontology, given its inherent complexity and the need for ongoing extensions due to the dynamic nature of the domain, characterized by frequent changes and constant development. To address this, it is recommended to frame the ontology under the open-world assumption (OWA) [218; 219]. This assumption accommodates incomplete information, acknowledging that there might be more pertinent details than are currently available. It proves advantageous for expressing knowledge in a manner that is adaptable and widely employed, particularly within the field of artificial intelligence. Our goal is to develop a domain ontology that allows for future extensions, aligning with the evolving nature of the domain.

The domain ontology named MIoT ontology provides a common understanding between two specific areas, i.e., remote patient monitoring (RPM) and cybersecurity. This cross-domain ontology shows how to detect vulnerabilities in remote patient monitoring systems by using semantic standards and technologies like RDF and OWL. By defining the resources, vocabularies, definitions, annotations, etc., related to medical devices in remote patient monitoring, vulnerabilities are detected that are ultimately exploited by attacks.

The ontology development process is divided into the five following stages shown in Table **??**. Specification and scope, existing ontologies reused, term enumeration, conceptualization, and formal grounding with description logics act as a foundation for this research work. This process involves the articulation of the knowledge area, the research's purpose, and the formulation of concepts, relationships, and axioms. MIoT is an informal ontology [207] where a conceptual model is presented in this paper.

Table 4.3: Ontology Development Process

Stages for Ontology Development
Specification and Scope
Reuse Existing Ontologies
Term Enumeration
Conceptualization
Formal grounding with Description Logics

4.4.1 Specification and Scope

Due to advancements in communication networks, the Internet of Things (IoT) has brought new directions in which a person can connect with any device from any location. The remote healthcare patient monitoring system is one example, where IoT devices can detect the patient's condition and whether they behave normally or not by checking their blood pressure, heart rate, etc. In case of any abnormal reading, it will alert the doctor or caregiver for assessment. While these IoT networks are very beneficial and attractive towards healthcare and the community, at the same time, there are also chances of the occurrence of security risks.

The specification signifies the importance of the ontology development process, which is descriptive and prescriptive [220] and notifies who is going to use the model and why [221]. Given the sensitivity of the healthcare domain to cyberattacks and vulnerabilities due to the exposure of heterogeneous data on the web, the primary goal is to enhance cybersecurity measures, ensuring patient safety and data integrity in remote monitoring environments. The proposed domain ontology seeks to systematically address vulnerabilities in medical devices utilized for remote patient monitoring within the healthcare domain. This involves developing a comprehensive understanding of interconnected concepts relevant to the medical setting, including medical devices containing actuators, medical sensors, their connectivity (e.g., Bluetooth or Wi-Fi), and associations with vulnerabilities, exploits, and supporting systems and networks. It incorporates a well-defined vocabulary (i.e., schema.org), including terms such as medical device, person, product, service, etc. The ontology features a hierarchical structure with defined classes and subclasses, such as person as a class with three subclasses: patient, doctor, and healthcare provider. Importantly, this ontology excludes non-medical IoT devices and vulnerabilities unrelated to healthcare. This phase establishes the foundation for the subsequent ontology development phase, which involves conceptualization.

4.4.1.1 Data Acquisition

The phase of acquiring knowledge plays a crucial role in the ontology-building approach from the ground up. It ensures the gathering of essential data for the design and population of the ontology. This research collects and observes data and information from diverse sources to ensure that the ontology is comprehensive, well-informed, and reflective of the current state of knowledge in the

domain of medical device vulnerabilities, particularly cybersecurity in healthcare in general. This approach enhances the ontology's ability to address real-world challenges and capture a wide spectrum of information relevant to the identification and management of vulnerabilities in medical devices for remote patient monitoring.

The formal representation of knowledge in a specific domain includes information derived from the specifications of medical devices such as technical details, functionalities, configurations, and any other relevant attributes (i.e., manufacturer information) that define the characteristics of these medical devices. Additionally, data from databases dedicated to cybersecurity e.g., National Vulnerability Database (NVD), is incorporated. These databases likely contain information about known vulnerabilities, threats, attack patterns, and countermeasures related to medical devices and healthcare systems. Information obtained from incident reports document instances of security breaches, cyberattacks, or other adverse events related to medical devices. Analyzing these reports helps in understanding real-world scenarios (i.e., ransomware) and identifying potential vulnerabilities (i.e., Log4J). Moreover, insights from the relevant literature, such as research papers, articles, and publications in the fields of medical device security, cybersecurity, and healthcare technology, are used. This includes academic studies, industry reports, and expert opinions that contribute to the knowledge base.

4.4.1.2 Competency Questions

(a) What types of devices are utilized in the IoMT environment?

(b) Who are the vendors of medical devices?

(c) What firmware, version, operating system, software, or applications are utilized in manufacturing medical devices?

(d) What kind of vulnerabilities are potentially presented in specific IoMT devices?

(e) Are any of the medical devices vulnerable in a remote patient monitoring setting?

(f) Which type of data is more sensitive to vulnerabilities/attacks?

(g) Which population is more affected? i.e., patients, doctors, administration, etc.

(h) What are the potential consequences and adverse side effects of identified vulnerabilities/attacks?

(i) What countermeasures should be implemented for specific vulnerabilities?

(j) *Ontology exclusion:* Which medical devices or vulnerabilities are not addressed in this ontology?

4.4.1.3 Answers to the Competency Questions

The IoMT environment integrates a range of devices, including actuators and medical sensors, facilitating remote patient monitoring. In our analysis, we identify vendors supplying medical devices crucial for remote monitoring, along with their specific configuration details. Notably, we exclude devices primarily utilized in clinical or hospital settings, such as surgical instruments. Utilizing ontology, we

conduct a thorough examination to assess the vulnerability status of these medical devices while also evaluating potential consequences. Consequently, we propose tailored countermeasures to address identified vulnerabilities accordingly.

4.4.2 Reusing Existing Ontologies

Reusing existing ontologies can significantly reduce the time and effort required for development and ensure alignment with industry standards. The choice of the most suitable ontology development approach depends on defining the starting point: whether to build the ontology by integrating existing ones or to create it from scratch [207]. Several existing ontologies in the domain of healthcare, medical devices, and cybersecurity were examined that could potentially be reused or serve as a foundation for developing a new ontology.

Our literature review indicates that existing security ontologies are typically either exclusively focused on vulnerabilities or cyberthreat aspects (IDS [203], IoTSec [205], UCO [215]) and rarely, if at all, integrate cybersecurity-health interactions.

Given the complexity and importance of these interactions in impact propagation studies, their formalization cannot be limited to merely combining the two separate domains. Moreover, the healthcare ontologies SNOMED CT [195], SafeCareOnto [222], and Medical Device Ontology (MDO) [215], among others, generally emphasize medical process terminologies or hospital settings and frequently neglect security considerations for remote patient monitoring environments.

4.4.3 The Term Enumeration

In the context of ontology engineering, the term ‘enumeration’ typically refers to a concept in which a specific property or attribute can take on one of a limited, defined set of values. These values are explicitly listed, and no other values are permitted for that property. Enumeration is a powerful tool in ontology engineering as it provides clarity and structure to the data model, ensuring that the ontology accurately represents the real-world domain it is intended to describe [212].

In the context of IoMT and cybersecurity, a few examples of terms used for MIoT ontology are: class (MedicalDevice, Vendor, Product, Person, Vulnerability, Exploit), subclasses (Actuators, MedicalSensor, Patient, Doctor, HealthcareProvider), Object properties (hasProduct, hasVenor, hasVulnerability, hasExploit, moniterdBy, effects), and data properties (hasName, hasSeverity, hasPublished). The next steps are developing a class hierarchy and defining the properties of these classes (concepts), called conceptualization.

4.4.4 Conceptualization

The conceptualization phase is very important in any software engineering development process. It defines the principles and design criteria to develop the domain ontology. Conceptualization involves organizing domain knowledge into a conceptual model that describes the problem and its solution using the vocabulary of the specific domain. By structuring information in this way, it becomes easier to understand and communicate complex concepts within the domain.

There are various approaches to developing a class hierarchy. Selecting the most appropriate approach for ontology development depends on determining the starting point, which involves deciding whether to build the ontology by integrating existing ontologies, reusing those ontologies, or creating it from scratch. As discussed in Section 4.4.2, the existing ontologies are not within our domain of scope, so we have adopted the scratch method to align with our project specifications. The 'from scratch' method [223; 224] includes top-down, bottom-up, and middle-out approaches. Top-down approaches entail identifying a core of abstract, generic concepts and expanding it through specialization into more domain-specific concepts. In contrast, bottom-up approaches involve capturing task specifications, gathering terms, and defining new concepts at a low level. These low-level concepts can later be generalized to a higher level. Middle-out approaches establish core concepts before deriving new ones through specialization and generalization based on expert data.

The top-down approach is used for ontology development in our work. The concepts, relations, and axioms are the primary elements. Various types of links connect concepts at higher levels, including equivalence links (synonyms), hierarchical links (inheritance), and associative links (associations/relationships). Each concept denotes a collection of distinct individuals, also referred to as instances. Axioms facilitate the definition of the semantics of concepts and relations, expressing certain constraints on their values or cardinalities. The incorporation of axioms allows for the representation of specific capabilities or features of a concept while preventing the introduction of new concepts that might not be reused [225]. This way, the information about IoMT, RPM, and vulnerabilities can be queried or updated by the corresponding people or applications. The conceptualization phase consists of a set of activities [217], such as:

(a) Identifying concepts and their instances, attributes, and corresponding values within a *Data Dictionary (DD)*.

(b) Organizing various concepts into hierarchical structures in *concept classification trees*.

(c) Detailing properties such as object properties and data properties of classes and instances in respective *Table of object properties* and *Table of data properties*.

(d) Recording specific instances in a *Table of Instances*.

4.4.4.1 Data Dictionary

The creation of a Data Dictionary (DD) marks the initial step in capturing domain knowledge. This essential document identifies and gathers relevant domain concepts, including their meanings, properties, instances, and other relevant details [226]. Each concept in the domain may be documented with fields such as concept name, synonyms and acronyms, concept description, instances of the concept, class attributes, and instance attributes. The resulting Data Dictionary is a comprehensive reference for understanding the domain. A few high-level concepts from MIoT ontology for DD are provided in Table 4.4, with some of their instances, class attributes, and instance attributes.

Table 4.4: Table for Data Dictionary

Data Dictionary Table				
Concept Name	**Description**	**Instances**	**Class Attributes**	**Instance Attributes**
Product	Refers to medical devices or other healthcare products	Medfusion4000-Pump, CRH[1], GMS[2]	affectedBy, hasVendor, monitor, attackedBy, monitoredBy, purchasedBy, usingCoonnectivity	hasVersion, hasName, hasSensorType, productID
Vendor	An entity that sells or supplies medical devices to healthcare organizations, hospitals, clinics, or patients	Abbott, SmithMedical, IHealth, MySignals, Foracare, Boston-Scientific, AliveTech	hasProduct, hasVendor	hasName, manufacturedID
Service	It is a communication pathway to transfer data between two devices	Bluetooth, CloudBased, Wi-Fi, MQTT, BLE	usingConnectivity, disruptsService, targetService, byUsingService,	hasBluetooth, hasName
Vulnerability	A vulnerability refers to a weakness or flaw in a system's design, implementation, or configuration that could be exploited by attackers to compromise the security of the system, its data, or its users	RemoteCode-Execution, BufferOver-flowVulnerability	hasVulnerability, exploitedBy, effectsOn, mitigate	vulnerabilityID, vulnerabilitySeverity, VulnerabilityVersion, hasImpactScore, hasExploitabilityScore, hasAvailability-Impact, hasConfidentialityImpact, hasIntegrityImpact, hasSeverity

[1]CardiacRhythmManagement. [2]GlucoseMonitoringSystem.

4.4.4.2 Concepts Classification Tree

After nearly completing the DD, the next step is to develop concept classification trees (CCTs). These trees are used in ontology building to organize domain concepts into taxonomies, forming a class/subclass hierarchy. These trees are not just for understanding relationships among concepts but also for dividing domain knowledge into independent, modular ontologies. The concepts described in

DD must be shown in the CCTs and vice versa. Figure 4.1 shows the concept classification trees for MIoT ontology.

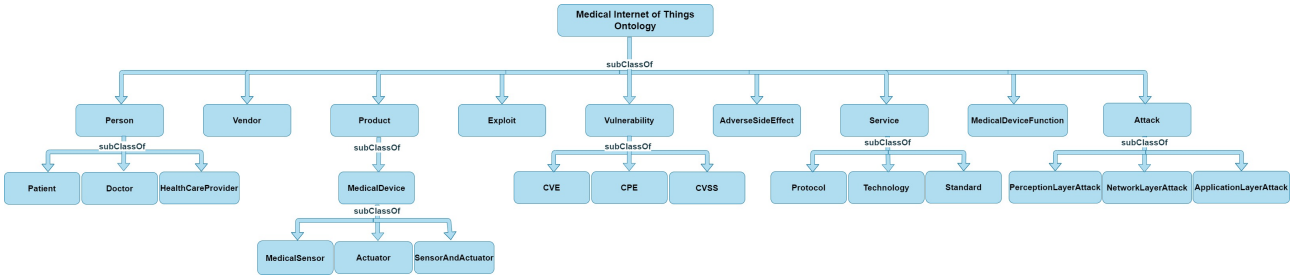

Figure 4.1: Class diagram for the Concept Classification Tree.

4.4.4.3 Table of Object Properties and Table of Data Properties

Furthermore, object and data properties are two fundamental types of properties used to describe the relationships and attributes of individuals (instances) in a domain. These properties are commonly used in knowledge representation and Semantic Web technologies. Object properties express relationships between concepts or instances in the ontology, while data properties are used to assign values to individuals, representing attributes or characteristics of instances using literal values (strings, integers, etc.).

(a) Examples of Object Properties

:MedicalDevice rdf:type owl:Class .
:Vulnerability rdf:type owl:Class .
:hasVulnerability rdf:type owl:ObjectProperty .

In this turtle example, MedicalDevice and Vulnerability are concepts and hasVulnerability is an object property.

:InsulinPump rdf:type :MedicalDevice .
:Heartbleed a :Vulnerability .
:insulinPump :hasVulnerability :Heartbleed .

In this turtle example, InsulinPump and Heartbleed are instances of ontology and hasVulnerability is an object property. The full list of object properties with their domain and range is given in Table 4.5

(b) Examples of Data Properties

:hasBloodPressure rdf:type owl:DatatypeProperty .
:BloodPressure rdf:type :MedicalDeviceFunction .
:BloodPressure :hasBloodPressure “120”^^xsd:int .

In this turtle example, BloodPressure is an individual and hasBloodPressure is a datatype property, and BloodPressure has a blood pressure value of at least 120.

:hasSeverity rdf:type owl:DatatypeProperty .
:RemoteCodeExecution rdf:type :Vulnerability .
:RemoteCodeExecution :hasSeverity “High”^^xsd:string .

In this turtle example, RemoteCodeExecution is an individual and hasSeverity is a datatype property, and RemoteCodeExecution has a high severity.

In these examples, RDF syntax is used to illustrate how ontological concepts can be represented. The terms like rdf:type, owl:Class, owl:ObjectProperty, and owl:DatatypeProperty come from OWL, which is commonly used for creating ontologies. The list of a few data properties with their domain and range is shown in Table 4.6. These data properties have been selected based on their relevance to the competency questions and their widespread usage in the fields of IoMT and cybersecurity.

Table 4.5: Table of object properties with their domain and range.

Object properties with their domain and range.		
Object Properties	**Domain**	**Range**
affectedBy	Product	Vulnerability
attackedBy	Product	Attack
byUsingService	Service	Person
causedBy	AdverseSideEffect	Attack
disruptsService	Attack	Service
effectsOn	Vulnerability	Product
exploitedBy	Vulnerability	Exploit
exploitsVulnerability	Attack	Vulnerability
hasAttack	Exploit	Attack
hasCredential	Patient	Product
hasProduct	Vendor	Product
hasVendor	Product	Person
hasVulnerabilty	Exploit	Vulnerability
Mitigate	Countermeasure	Vulnerability
Monitor	MedicalDevice	MedicalDeviceFunction
monitoredBy	Product	Vendor
Protect	Countermeasure	Product
purchasedBy	Product	Patient
targetService	Attack	Service
usingConnectivity	Product	Service
usingDevice	Patient	Product
usingService	Patient	Service

Table 4.6: Table of data properties with their domain and range.

Data properties with their domain and range.		
Data Properties	**Domain**	**Range**
attackType	Attack	String
hasAccessComplexity	Vulnerability	String
hasAccessVector	Vulnerability	String
hasAttack	Attack	String
hasAuthentication	Vulnerability	String
hasAvailabilityImpact	Vulnerability	String
hasBaseScore	Vulnerability	String
hasBloodPressure	MedicalDevice	Integer
hasBluetooth	Technology	String
hasDosageValue	MedicationDosage	Decimal
hasModifiedData	NetworkLayer	Boolean

4.4.4.4 Table of Instances

Based on the scope and domain of the ontology, and after defining the concepts and relationships, gathering instances that represent these concepts in the real world is important. These instances should be diverse yet typical, covering various aspects of the domain. Additionally, ensuring the relevance of selected instances is essential; they should accurately illustrate the characteristics and behaviors of the concepts they represent. Considering the potential use case or application of the MIoT ontology, such as for vulnerability detection in remote patient monitoring, the instances are defined to demonstrate the functionality and utility of the ontology in practical scenarios.

After finalizing all instances (individuals) listed in the 'Instance' field of the Data Dictionary (DD) within the domain, the subsequent step involves creating a table of instances for each instance identified in the DD. An example of such a table is illustrated in Table 4.7. This process involves the instance name, description, and related concepts.

Table 4.7: Table of instances and their description.

Instances and their description.		
Instance Name	**instanceOf**	**Description**
Medtronic [1]	Vendor	is a vendor of medical devices
BloodPressureMonitor	SensorAndActuator	is a medical device used to measure and monitor a person's blood pressure

Continued on next page

Table 4.7 – continued from previous page

Instance Name	instanceOf	Description
BufferOverflowVulnerability	Vulnerability	is a type of security flaw or weakness in a computer program
CardiacRhythmManagement	Product	are designed to diagnose, manage, and treat disorders related to heart
HealthCondition	MedicalDeviceFunction	refer to a condition related to health
InfusionPump	Actuator	utilized to introduce fluids, medications, or nutrients into the circulatory system of a patient.
LifeThreatening	AdverseSideEffect	a situation where a danger occurs to someone's life.
MQTT	Protocol	is a messaging protocol and well-suited for communication between devices with limited resources, such as sensors and actuators.
Wi-Fi	Technology	is a set of wireless communication standards used for transmitting data between devices over short distances such as medical devices.

[1] `https://www.medtronic-diabetes.com.au/`[Accessed on 10 March 2022].

4.4.5 Formal Grounding with Description Logics

Formal grounding is a subsequent process that involves explicitly and logically defining concepts (classes), roles (relationships), and individuals (instances). In the realm of knowledge representation, formal grounding ensures the consistency, logic, and utility of the ontology for inference purposes. This approach facilitates sophisticated reasoning and querying capabilities within ontologies [227; 228]. The hierarchical arrangement within the knowledge domain of the ontology, shown in Figure 4.1, has been formally established using a description logic formalism with an expressivity of $ALO^{(D)}$. Some examples of concepts, roles, and individuals within the ontology comprise the following three headings:

4.4.5.1 Concepts Hierarchy in Description Logic

One fundamental aspect of formal grounding is the development of a concept hierarchy using description logic (DL) axioms. This hierarchy organizes concepts in a structured set of concepts (classes) and their relationships in a formal, logical manner. In the context of ontologies, a concept hierarchy is a way of organizing knowledge where more general concepts are at higher levels and more specific concepts are at lower levels. In DL, this is primarily achieved using subclass relationships. Key elements in concept hierarchy with DL axioms are given here:

- Concepts (Classes): In DL, concepts are the basic units and represent sets of individuals (or objects). They are denoted by capital letters and singular. For example, Vulnerability, Person, and Actuator are shown as an example in Figure 4.1.
- Subclass relation: The subclass relation $\sqsubseteq$ is used to define a hierarchy between concepts. If A $\sqsubseteq$ B, it means every instance of concept A is also an instance of concept B. For instance, MedicalSensor $\sqsubseteq$ MedicalDevice indicates that medical sensors are medical devices.
- Top and bottom concepts: Top ($\top$) or universal concepts and bottom ($\bot$) concepts are used to denote the broadest and the most restricted scopes, respectively. For example, $\top$ could be used to denote a concept that is too general or unspecific, and it includes all individuals. Meanwhile, $\bot$ can be used to represent an impossible or contradictory concept and includes no individuals.

Concept hierarchy is started by defining basic concepts such as:

MedicalDevice, Vulnerability, Exploit, Target, Person etc.

Specific concepts are then created and defined in their relationship to the general ones by defining subclass relationships such as:

Patient $\sqsubseteq$ Person, MedicalDevice $\sqsubseteq$ Product, MedicalSensor $\sqsubseteq$ MedicalDevice, Technology $\sqsubseteq$ Service etc.

Furthermore, define concepts with restrictions, like property restrictions or cardinality constraints, for instance.

MedicalDevice $\sqsubseteq\exists$ usingConnectivity. Technology

This axiom shows that 'Every instance of MedicalDevice is associated with at least one instance of Technology through the usingConnectivity property.', where

'MedicalDevice' refers to the class of Product.

'$\sqsubseteq$' denotes subclass or subclass relationship.

'$\exists$' denotes existential quantification, meaning 'there exists.'

'usingConnectivity' is a property that relates a medical device to a technology.

'Technology' refers to the class of service.

4.4.5.2 Role Definition in Description Logic

In DL, these properties are called roles, i.e., object role and data role. An object role is typically defined as a binary relation. For example, if R is an object role and a and b are individuals, then R(a, b) means that there is a relationship R between a and b. In MIoT ontology, e.g., hasVulnerability (bloodPressureMonitor, heartBleed), hasVulnerability is an object, i.e., R, and bloodPressureMonitor and heartBleed are individuals. It shows that bloodPressureMonitor has a vulnerability named heart bleed. Meanwhile, a data role links an individual to a data value. For example, if D is a data role, a is an individual, and v is a data value, then D(a, v) indicates that the individual a has a data property D with value v. For instance, monitor (Pacemaker, HealthCondition) would mean that Pacemaker is used to monitor health condition. Roles can be restricted using existential quantification (∃R.C, meaning there exists a relationship R to an individual of class C) or universal quantification (∀R.C, meaning all relationships R lead to individuals of class C). For example, existential quantification ∃ in formal logic, shown as

$$\text{MedicalDevice} \sqsubseteq \exists \text{hasVulnerability. Vulnerability.}$$

It shows that every instance of MedicalDevice is associated with at least one instance of Vulnerability through the role hasVulnerability.
In turtle format:

```
:MedicalDevice rdf:type owl:Class .
:Vulnerability rdf:type owl:Class .
:hasVulnerability rdf:type owl:ObjectProperty .
:MedicalDevice rdf:subClassOf [
rdf:type owl:Restriction ;
owl:onProperty :hasVulnerability ;
owl:someValuesFrom :Vulnerability ].
```

Similarly, universal quantification ∀ in formal logic is shown as:

$$\text{MedicalDevice} \sqsubseteq \forall \text{ hasExploit. Exploit.}$$

It shows every instance of MedicalDevice is associated with only instances of Exploit through the role hasExploit.
In turtle format:

```
:MedicalDevice rdf:type owl:Class .
:Exploit rdf:type owl:Class .
:hasExploit rdf:type owl:ObjectProperty .
:MedicalDevice rdf:subClassOf [
rdf:type owl:Restriction ;
owl:onProperty :hasExploit ;
owl:allValuesFrom :Exploit ].
```

4.4.5.3 Individual Declarations

In DL, the formal grounding of individuals provides a foundation for accurately and consistently representing specific entities and their relationships within an ontology. In the context of formal grounding, individual-related assertions follow the syntax and semantics of description logic, such as:

- *MedicalSensor(pacemaker)* states that pacemaker is an individual of the class *MedicalSensor*.
- In another axiom, *monitor(pacemaker, healthCondition)* could represent that pacemaker monitors health condition.

Assertions can also be more complex, involving roles and role restrictions. For example,

$$\exists monitor.MedicalSensor(pacemaker)$$

indicates that the pacemaker monitors at least one object of the class *MedicalSensor*.

Based on the defined individuals and their relationships, the reasoning engine infers new knowledge, checks for inconsistencies, and answers complex queries.

4.5 Developing the Conceptual Model for MIoT Ontology

The conceptual model for MIoT ontology, named the MIoT model, provides a centralized repository and utilities that all participants in this system can share and communicate effectively. This will speed up the development process, foster interoperability, and improve the correlation of test results. The model is based on the proposed methodology (KEM), where concepts, their properties, and relationships are defined.

4.5.1 Detailed Description of MIoT Model

The main ideas in MIoT (Medical Internet of Things) ontology are interconnected (concepts) through various properties (relationships), serving different purposes within the scope of the Internet of Medical Things (IoMT) and addressing various scenarios and use cases. For example, a medical device (such as an insulin pump) monitors a device function (such as glucose level), manufactured by a vendor (such as XYZ) and monitored by a person (such as the patient). A vulnerability that exists in the product (such as the Heartbleed Vulnerability), can be exploited by an attack (such as a DDoS attack) due to using a service (such as Wi-Fi), leading to adverse effects. Countermeasures can then be applied to protect the product by mitigating the vulnerability. This is a simple use case addressed by our model. Researchers can perform rule-based reasoning on the proposed model to address more comprehensive use cases. Figure 4.2 below illustrates the MIoT model where each high-level concept and their related properties are described.

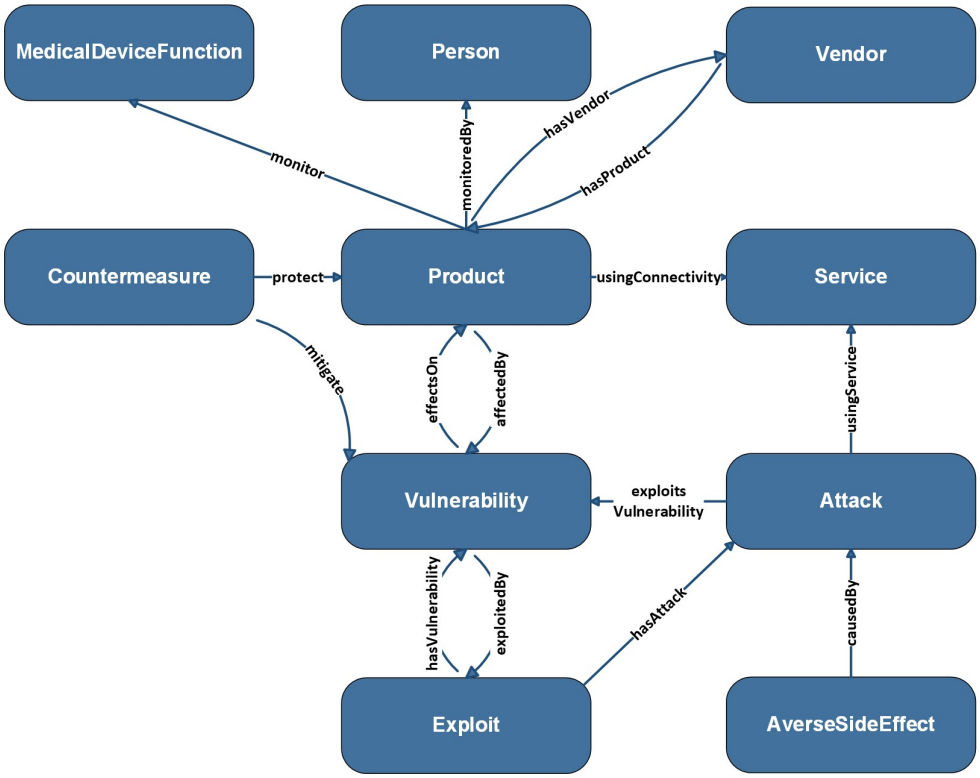

Figure 4.2: The Conceptual model of MIoT ontology.

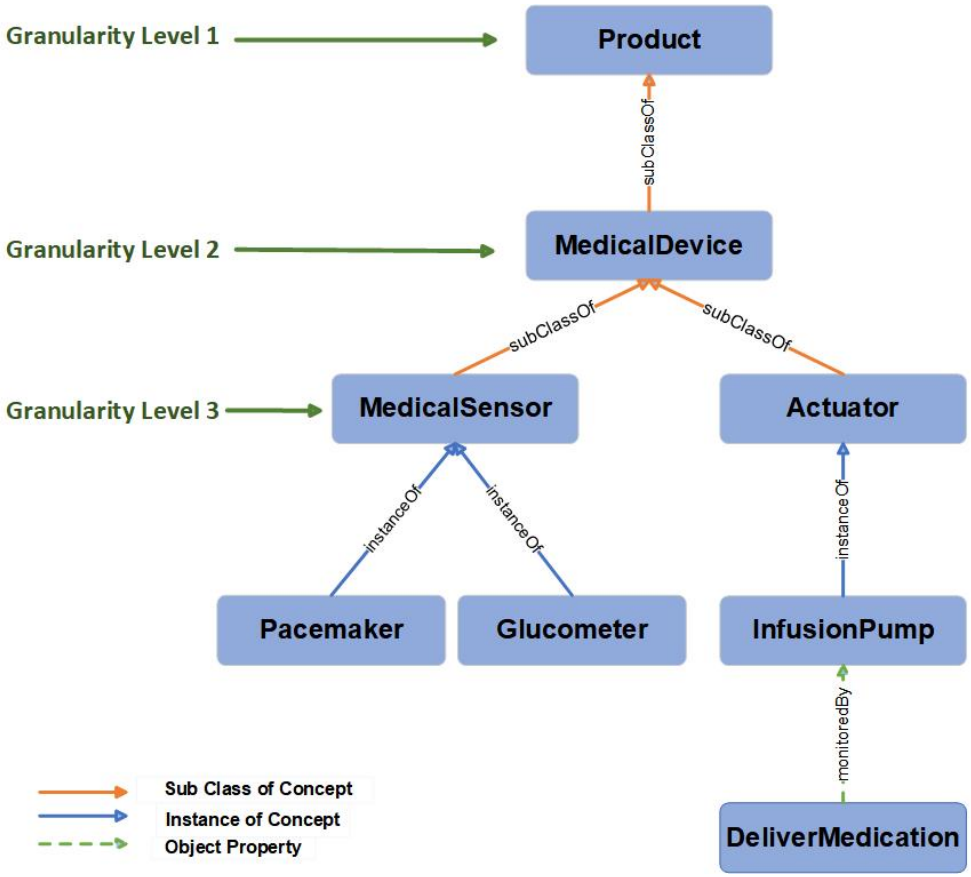

Figure 4.3: The granularity of MIoT ontology described for the concept `Product` with subclasses, instances, and relationship.

The MIoT ontology is designed to articulate concepts not only at a high level but also to reach deeper level, spanning across three distinct levels of granularity. At Level 1, foundational concepts such as Product, Vulnerability, Exploit, Person, and Service are established. Level 2 extends this framework to include domain-specific entities, listed as terms such as Medical Device, Patient, Healthcare Provider, and Technology. Finally, Level 3 refines the ontology with specialized subclasses such as Medical Sensor and Actuator. A detailed illustration is shown in Figure 4.3 describing the hierarchical design of the concept product with its subclasses across these three levels.

It is worth noting that the lower-level occurrences are facilitated through rule-based reasoning, which are security elements that fall beyond the scope of this current paper. Fundamental expressions such as 'product', 'medical device', 'patient', and 'healthcare provider' describe the IoMT entities, while terms such as 'vulnerability', 'exploit', 'attack', and 'countermeasure' define the crucial roles that characterize the various security vulnerabilities. Details about descriptions, properties, and instances are discussed in the Data Dictionary table.

4.5.2 Case Study

To define the problem domain clearly and discuss the concepts, relationships, and constraints involved in the MIoT ontology and evaluate the performance, a hypothetical scenario is presented here, which is adopted from the Digital Living Lab [229].

Suppose we have scenario *X*; John, a patient managing hypertension. He relies on a comprehensive remote patient monitoring system, which includes a blood pressure monitor and a diabetes management tool. However, upon noticing alarming blood pressure readings, he alerts his doctor, leading to the discovery of a network vulnerability. An attacker exploited this vulnerability, compromising the accuracy of John's readings and causing serious risks to his health. The doctor immediately takes steps to address the issue and ensure that John's monitoring system is secure. They also advise John to continue monitoring his blood pressure manually until the issue is resolved.

Despite these efforts, further complications arise when John's infusion pump used for medication administration is also compromised weeks later. An attacker gains access to the pump's network connection, altering medication dosages and resulting in severe adverse effects for John, requiring hospitalization. This incident underscores the critical need for secure remote patient monitoring systems, emphasizing the imperative of protecting medical devices from vulnerabilities and ensuring patient safety. There is a need to automate the system that takes security measures and alarms the patient and healthcare providers about the vulnerabilities in the system. It must be implemented to mitigate risks associated with vulnerabilities exploited by attacks, safeguarding the accuracy and integrity of medical device data transmission through the network.

In terms of vulnerability detection, this work develops assumptions based on scenario x. The generated assumptions from the provided hypothetical scenario would focus on vulnerability identification and its consequences on patients, medical devices, and data and propose countermeasures to mitigate attacks that exploit vulnerabilities.

4.5.2.1 Assumptions

1. Medical devices for remote patient monitoring systems from a Vendor utilize network connectivity to transmit data to healthcare providers.

2. Due to the attack, data are modified and transmitted between the medical device and the healthcare provider through the network layer, compromising the confidentiality and integrity of the patient's information.

3. Vulnerabilities in the network layer of remote patient monitoring systems may lead to inaccurate readings or manipulation of medical data.

4. The compromise of medical devices, such as infusion pumps, due to vulnerabilities in their network layer, can have severe consequences, including adverse side effects for patients and the need for hospitalization to address medication-related issues.

5. The incident with John's infusion pump underlines the importance of implementing robust security measures in remote patient monitoring systems to safeguard against potential attacks and vulnerabilities that could risk patient safety and compromise the accuracy of medical data.

4.5.3 Evaluation

Identifying potential weaknesses and vulnerabilities during the design phase is crucial for establishing robust security measures from the beginning. Formal methods offer a promising way to determine such flaws at an early stage. Through formal verification and validation techniques, reliability and security can be assured, assessing the accuracy of designs using diverse mathematical and logical methods [230; 231]. Furthermore, formal methods identify design errors early in the development process and ensure that the system aligns with specifications, requirements, and standards [232].

Formal methods, such as mathematical and logical notations, employ automated tools to analyze the behavior and properties of the system, including tasks such as checking for consistency, completeness, and correctness [233]. In our research, we use logical methods, more specifically, symbolic logic (i.e., propositional logic). In propositional logic, axioms are statements that define relationships or properties within an ontology to satisfy the given assumptions. For the given assumptions, we write the axioms in the form of propositional logic and define the notations representing the concepts in the MIoT ontology, as shown in Table 4.8.

Assumption 1. These axioms define the relationships between the medical devices, vendors, network connectivity through the network layer, and healthcare provider in the context of the remote patient monitoring system.

$$\texttt{manufacturedBy(Med1, V)} \wedge \texttt{manufacturedBy(Med2, V)}$$
$$\texttt{usingConnectivity(Med1, NL)} \wedge \texttt{usingConnectivity(Med2, NL)}$$
$$\texttt{receiveData(HP, NL)}$$

Table 4.8: Notations for Concepts and their description used in Scenario X.

Notations for Concepts and Description	
Notations for Concepts	**Description**
A	Attack
ASE	Adverse side effect
C	Countermeasure
H	Hospitalization
HP	Healthcare provider
MD	Medical device
MD1	Type of medical device (i.e., BP monitor)
MD2	Type of medical device (i.e., Infusion pump)
NL	Network layer
P	Patient
V	Vendor
Vul	Vulnerability

Assumption 2. These axioms define the relationships between attack, medical device, network connectivity, healthcare provider, and patients' information, specifying the actions that attackers may take and their potential consequences in compromising the integrity and confidentiality of patients' information.

$$\texttt{Attack(A)} \land \texttt{interceptsData(A,MD,HP)} \land \texttt{hasModifiedData(NL,true)} \rightarrow \texttt{compromisesIntegrity(P)} \land \texttt{compromisesConfidentiality(P)}$$

Assumption 3. These axioms define the relationships between vulnerabilities in the network layer, inaccurate readings, or manipulation of medical data, specifying the potential consequences of network vulnerabilities in the remote patient monitoring system.

$$\texttt{Vulnerability(Vul)} \land \texttt{inNetworkLayer(V,NL)} \rightarrow (\texttt{inaccurateReadings(NL)} \lor \texttt{manipulationOfMedicalData(NL)})$$

Assumption 4. This axiom states that if a medical device has a vulnerability and is connected to a network layer, then this vulnerability can lead to adverse side effects for patients and requires hospitalization to address medication-related issues.

$$\texttt{MedicalDevice (MD)} \land \texttt{hasVulnerability(MD,Vul)} \land \texttt{connectedTo(MD,NL)} \rightarrow \texttt{causedAdverseSideEffect (A,ASE)} \land \texttt{requiresHospitalization(ASE,H)}$$

Assumption 5. If there is an incident with John's infusion pump, this axiom emphasizes the importance of taking countermeasures to implement robust security measures, which in turn helps prevent potential attacks and ensures the accuracy and integrity of medical data in remote patient monitoring systems.

$$\texttt{takeCountermeasure(C)} \rightarrow \texttt{implementRobustSecurityMeasures(C)} \wedge \texttt{preventAttack(MD2,C)} \wedge \texttt{preventInaccurateReadings(NL,C)} \wedge \texttt{preventManipulationOfMedicalData(NL,C)}$$

In summary, the evaluation of this case study demonstrates that the proposed model strongly aligns with a system that addresses the key concerns relevant to the areas of interest in this solution. The case study illustrates the model's effectiveness in addressing critical issues such as confidentiality and integrity. It indicates that assumptions based on a logic-based approach are effective in detecting and responding to key vulnerabilities, especially those occurring at the network layer, as evidenced by the majority of attacks in the presented case study.

4.6 Limitations and Future Work

This MIoT model aims to identify security issues, such as vulnerabilities, in the IoMT scenario from the perspectives of patients, doctors, and healthcare providers. While it is acknowledged in different literature [15; 234; 235] that caregivers are also part of IoMT, this aspect is not addressed in this work. Our focus is on those who directly interact with IoMT devices. To address this limitation, future work will include caregivers or other related stakeholders, such as pharmacists and accountants in the IoMT domain. Another challenge faced by researchers is the lack of publicly available datasets or real-time sensor data that address security issues such as vulnerabilities or cyberattacks in IoMT. To cope with this challenge, this work adopted a case study approach to validate our work.

The MIoT ontology has significant potential to revolutionize security automation within healthcare applications by providing a structured framework for representing and understanding the relationships among medical devices, vulnerabilities, and network infrastructure. Building upon the predefined concepts and relationships within the MIoT ontology, we aim to introduce automation capabilities within MIoT ontology through case studies for vulnerability analysis and reasoning. For this purpose, we will establish rules to enable automated reasoning to make more effective inferences and high-level decisions. To evaluate our results, the standardized vulnerability information provided by NVD in terms of CVE and CVSS (Common Vulnerability Scoring System) will be integrated with the MIoT ontology for the assessment and management of security vulnerabilities across various medical devices. This conceptual model will be implemented, visualized, and queried in a knowledge graph to store CTI (cyberthreat intelligence) for semantic representation and data integration.

4.7 Conclusions

An ontology serves as a structured and formal representation of knowledge, providing enhanced tools for communication, reusability, and knowledge organization. Semantic technologies not only facilitate communication and representation but also lay the groundwork for reasoning and decision making by enabling computers to understand the meaning (semantics) behind data. The focus of this research paper is to develop the MIoT ontology, which captures knowledge from two cross domains (i.e., IoMT

and Cybersecurity) and facilitates the interconnections between remote patient monitoring and security infrastructure, where vulnerability detection takes place.

While numerous publications explore into the application of semantic technologies in cybersecurity and healthcare, to the best of our knowledge, the MIoT ontology is a novel ontology expressly crafted for vulnerability detection in the remote patient monitoring setting. This ontology outlines fundamental concepts for vulnerability detection in remote medical devices, explaining their properties and defining their relationships through the utilization of knowledge engineering methodology. To add weight to our overall conclusion regarding the effectiveness of this proposed solution, the MIoT model underwent validation against a representative case study, demonstrating strong alignment with the model's vulnerability detection through the formal logic of an axiom-based approach.

Chapter 5

Knowledge Organization System for Partial Automation to Improve the Security Posture of IoMT Networks

Based on MIoT ontology development, a prototype has been created. This prototype includes concepts related to IoMT and cybersecurity, and it defines object and data properties using standard formalisms like RDF and OWL. Automated reasoning was performed to validate a hypothetical scenario. The details of this prototype development has been published in *Elsevier* [135] as a research article, and it is available online at:`https://doi.org/10.1016/j.procs.2023.10.342`.

Abstract

Remote patient monitoring is a healthcare delivery model that uses technology to collect and transmit patient data from a remote location to healthcare providers for analysis and treatment. Remote patient monitoring systems rely on a network infrastructure to gather and transmit data from patients to healthcare providers through a network. While these systems become more prevalent, they may also become targets for cyberattacks. This paper deals with the development of a domain ontology to facilitate partial automation to improve the security posture of IoT networks used in remote patient monitoring. For this purpose, it captures the semantics of the concepts and properties of the main security aspects of IoT medical devices. This is complemented by a comprehensive ruleset evaluated by using SPARQL queries, and automated reasoning over the aggregated knowledge.

5.1 Introduction

Over the last two decades, advancements in information and communication technology have enabled the design and development of real-time healthcare solutions. The COVID-19 pandemic has accelerated the implementation of such systems, particularly for those living with chronic medical conditions (diabetes, cardiovascular disease, etc.). In this regard, the Internet of Medical Things (IoMT) has played a pivotal role in connecting patients with doctors and hospitals. IoMT is the collection of IoT technologies, which monitor a patient's health and transmit the information through a network to a cloud server [37]. Remote Patient Monitoring (RPM) is one of the applications of IoMT, where a

continuous stream of real-time information about patients can be transferred through medical devices connected with IoT sensors. This allows healthcare providers to monitor patients' health status and manage their care remotely, without the need for in-person visits [39]. On the other hand, these medical devices face security breaches due to a lack of standard protocols defined by regulatory bodies and manufacturers.

The security concern in healthcare is shown by the enhanced market of the Internet of medical things (IoMT) which would be estimated at up to $158 billion in 2022, which was $41 billion in 2017 [41]. A recent report by The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Journal, published on March 15, 2023 [46], highlighted a concerning trend of data breaches affecting over 4 million patients. These breaches compromised sensitive information, including financial accounts, social security numbers, and medical treatment details. Similarly, according to the Australian Cyber Security Centre (ACSC)[1], hospitals and aged care facilities have become prime targets for cybercriminals, The COVID-19 pandemic shows a significant increase with an alarming rise in malicious cyber activities employing Maze ransomware specifically within the healthcare sector. Consequently, patients' health, along with the financial and personal data of both patients and healthcare institutions, faces high risks.

In this way, IoMT in remote patient monitoring faces many challenges in terms of heterogeneity and interoperability. Knowledge organization systems (KOS) are among those solutions that support and organize data obtained from different sources. A KOS is a systematic and organized way for information retrieval, access, and use of knowledge resources. KOS include various types of taxonomies, ontologies, thesauri, and other controlled vocabularies [7]. KOS can be used to identify and manage patients' data and provide standardized terminology by capturing the semantics of their medical devices and their properties. KOS can also incorporate ethical guidelines and policies relevant to the use of IoMT in healthcare. This includes principles of privacy, informed consent, data security, and responsible data sharing. By embedding ethical principles [236] within the knowledge organization framework, healthcare providers, device manufacturers, and researchers can adhere to best practices and ensure the ethical use of IoMT devices and data. In such a way, semantic models can be used to represent medical information and knowledge in a structured and machine-interpretable format, which facilitates the sharing and integration of information among various systems. For example, an ontology can improve the interoperability of different IoMT devices, allowing for efficient and standardized communication between devices and systems. This can, in turn, be used, for example, for identifying device reading anomalies or unusual traffic, potentially linked to security issues.

In this article, MIoT Ontology is proposed for the semantic representation of medical IoT devices. SWRL rules are utilized to deduce the security aspects of IoT medical devices. The rest of the article is organized as follows: Section 5.2 describes the related work for knowledge organization systems; Section 5.3 provides the proposed ontology, and the conclusion is provided in the last section 5.4.

[1]https://www.cyber.gov.au/acsc/view-all-content/advisories/2020-013-ransomware-targeting-australian-aged-care-and-healthcare-sectors

5.2 Related Work

Many researchers work with knowledge organization systems where they deal with medical devices, various sensors, standards etc., to provide benefits to patients, doctors, and healthcare providers. To promote interoperability in the healthcare sector, an IoT-based system for collecting, integrating, and interconnecting IoT data in medical emergency services [108]. For this purpose, a semantic data model has been proposed that can uniformly store and interpret diverse IoT data. This method for accessing IoT data is effective in distributed heterogeneous environments, enabling prompt access to data on mobile and cloud computing platforms. To tackle the challenge of device heterogeneity, a mechanism has been developed by integrating and understanding the application programming interfaces (APIs) of different medical devices to collect their data [32]. This method utilizes an approach for constructing ontologies of the various APIs from both known and unknown medical devices and identifying their syntactic and semantic similarity with the help of mapping techniques.

A semantic model was proposed based on an IoT platform named SM-IoT [66]. This model facilitates interoperability between medical devices and data sources and includes contract-based security policies to ensure the confidentiality of patient health data. In our research, an ontology is developed based on expert knowledge in the domain of remote patient monitoring systems. This ontology detects compromised medical devices and performs automated reasoning.

5.3 A Proposed MIoT Ontology

In this research, the knowledge engineering methodology described in Ontology Development 101 [212] has been applied. By applying ontology engineering best practices, expert knowledge of the vulnerabilities of the medical IoT devices domain has been captured in a novel ontology called the MIoT Ontology . Beyond the concepts and roles of this domain, the MIoT Ontology also defines a ruleset to facilitate automated reasoning over the device reading anomalies or unusual traffic, potentially linked to security issues in medical smart home settings that use remote patient monitoring.

5.3.1 Specification and Scope

The scope of the proposed ontology has been set to cover all the concepts relevant to the semantic modeling of the remote patient monitoring device vulnerabilities domain. To this end, the terminology of both the underlying IT infrastructure and the corresponding device and technology has been covered. The MIoT ontology focused on those participants who are relevant to a remote patient monitoring system such as Patients, Doctors, Nurses, and caregivers. This Ontology shows how to capture the semantics of a remote patient monitoring system by using semantic standards such as RDF. Furthermore, the relationship between entities is defined in domain ontology, is based on various sources, and tackles the information in terms of medical devices, their connectivity, and their vulnerabilities.

5.3.2 Conceptualization

The taxonomical structure of the knowledge domain of the ontology has been formally grounded in a description logic formalism that has an expressivity of $ALO^{(D)}$. Some examples of concepts and roles of the ontology include:

(a) Concepts

AdverseSideEffect, Attack, NetworkLayer, MedicalDeviceFunction, MedicationDosage, Person, Patient, Product, MedicalDevice, BloodPressureReading, Target, Vendor, Vulnerability, weakness, etc.

(b) Roles

i. ***Object Properties:*** attackedBy, attackedOn, connectedToNetwork, hasDeviceType, hasPatient, hasVendor, hasVulnerability, hasCWE, etc. Table 5.1. shows all the object properties and their domains and ranges.

Table 5.1: List of Object Properties with their Domain and Range

Object Properties with their Domain and Range		
Object Properties	**Domain**	**Range**
attackedBy	MedicalDevice	Attack
attackedOn	Attack	Target
connectedToNetwork	MedicalDevice	NetworkLayer
hasAffectOn	Vulnerability	MedicalDevice
hasDeviceType	MedicalDevice	BloodPressureReading
hasPatient	MedicationDosage	Patient
hasTakenBy	Countermeasure	Vendor
hasVendor	Product	Vendor
hasVulnerability	MedicalDevice	Vulnerability
monitor	MedicalPerson	Patient
OccuredBy	AdverseSideEffect	MedicationDosage
protects	Countermeasure	Product
usingConnectivity	MedicalDevice	Service

ii. ***Data Properties:*** hasReadingValue, hasDosageValue, hasModifiedData, hasVulnerabilityID etc., the list of domains and ranges for the data properties are shown in Table 5.2.

Table 5.2: List of Data Properties with their Domain and Range

Data Properties with their Domain and Range		
Data Properties	**Domain**	**Range**
hasReadingValue	MedicalDevice	Decimal
hasAttack	NetworkLayer	String
hasAvailabilityImpact	Vulnerability	String
hasBaseScore	Vulnerability	String
hasIntegrityImpact	Vulnerability	String
hasConfidentialityImpact	Vulnerability	String
hasVulnerabilityID	Vulnerability	String
hasBloodPressure	MedicalDevice	Integer
hasBluetooth	Technology	String
hasDosageValue	MedicationDosage	Decimal
hasModifiedData	NetworkLayer	Boolean
hasName	Patient	String
hasCWEID	Weakness	String

iii. ***Datatype Properties:*** The de facto standard XSD datatypes (String, Integer, Decimal, Boolean) are used for the datatype properties of the ontology

(c) Individuals

John, Glucometer, LifeThreatening, BloodPressureMonitor, BloodPressureReading1, BloodPressureReading2, BloodPressureReading3, Wi-Fi, Cloud, etc.

5.3.3 Implementation

This Ontology has been implemented in OWL using Protégé 5.6.1, serialized in RDF/Turtle . The Protégé is an open-source software tool used for building knowledge-based systems, including ontologies. The MIoT Ontology uses the top-down approach where classes are divided into subclasses hierarchically shown in Figure. 5.1.

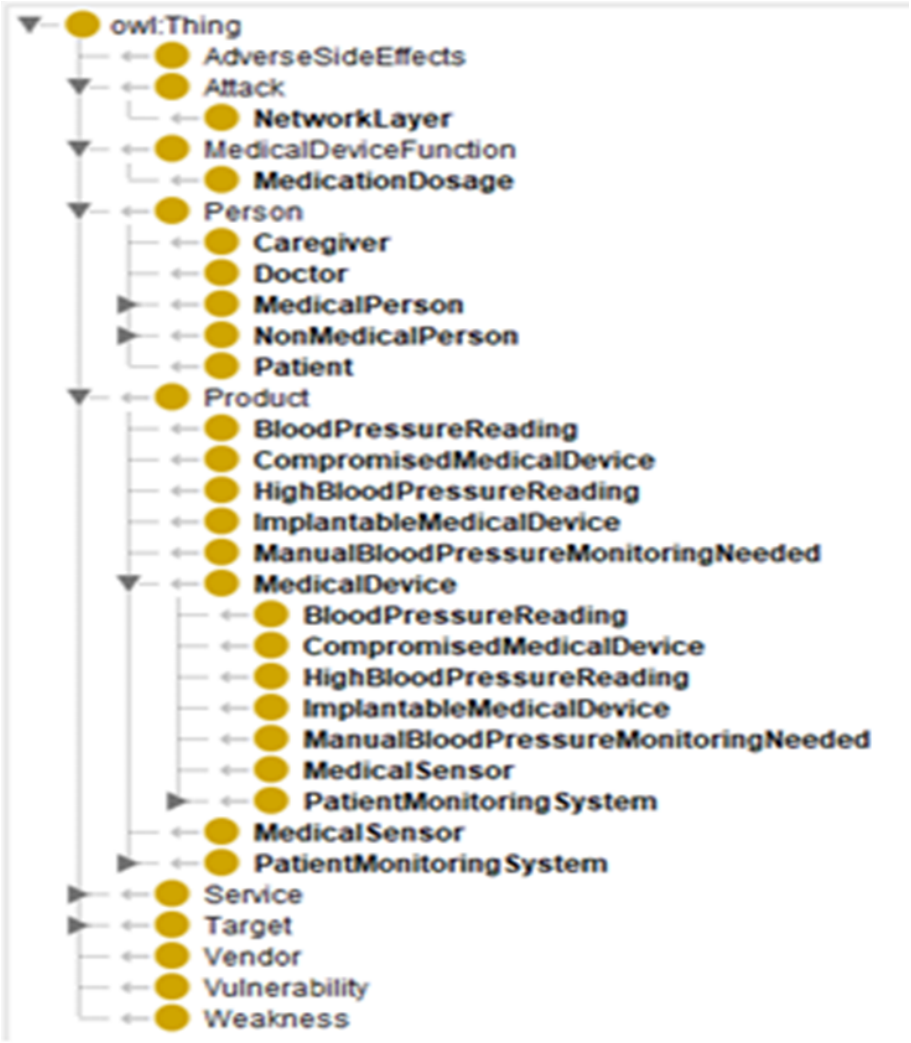

Figure 5.1: The hierarchical concepts for MIoT ontology.

5.3.4 Ruleset

To extend the expressivity of the ontology, a ruleset has been created. This can be used for reasoning over cyber-knowledge of remote patient monitoring device vulnerabilities. Among other things, it is suitable for:

(a) determining whether the reading of the blood pressure monitor derives from the normal value range;

(b) identifying if the medicine dosage has potentially been tampered with;

(c) generating the adverse effects if medication dosage is modified;

(d) recommending manual reading for the blood pressure monitor if it is likely to be compromised to manipulate medication dosage.

The inference rules are specified in SWRL (Semantic Web Rule Language) language.

Rule 1: If the system is vulnerable and the reading of the blood pressure monitor diverges from normal, this rule checks whether the blood pressure reading is higher than 120 (120/80 is a normal blood pressure reading) and infers a High Blood Pressure Reading.

```
BloodPressureReading(r), hasReadingValue(r, reading),
        greaterThan(reading, 120)
    → HighBloodPressureReading(r)
```

Rule 2: If a medical device such as a medication dosage is connected to the network and its data is modified due to a vulnerability, it infers that the device is a Compromised Medical Device.

```
MedicalDevice(d), connectedToNetwork(d, networklayer),
        hasModifiedData(networklayer,
true), hasVulnerability(d, vuln) → CompromisedMedicalDevice(d)
```

Rule 3: The adverse side effects are detected by checking if a MedicationDosage has a dosage value greater than 10 (The dosage value is between 5-8 in the system) and infers that Adverse Side Effects may occur.

```
MedicationDosage(d), hasPatient(d, p), hasDosageValue(d, dosage),
        greaterThan(dosage, "10")
        → AdverseSideEffect(p)
```

Rule 4: If a medical device such as a blood pressure monitor is compromised, this rule infers that Manual Blood Pressure Monitoring is needed for the patient until the issue is resolved.

```
CompromisedMedicalDevice(d), hasDeviceType(d,
        "Blood Pressure Monitor")
    → ManualBloodPressureMonitoringNeeded(d)
```

5.3.5 Evaluation

There are many reasoning engines available for ontology models such as Jena[2], Fact++[3], Racer[4], HermiT[5], Pellet[6], and so on. In this research, the Pellet reasoner is used to evaluate the consistency of the ontology. Pellet is an OWL-DL reasoner that offers extensive middleware and several unique features while achieving acceptable to very good performance. Additionally, it implements several OWL-DL extensions, such as a combination formalism for OWL-DL ontologies, and preliminary support for OWL/Rule hybrid reasoning [32].

After validation of ontology, it can be queried by users to deduce the implicit facts. The SPARQL query language allows extracting the knowledge from MIoTontology. Here we present some queries along with their results and description.

[2]https://jena.apache.org/documentation/inference/
[3]http://owl.cs.manchester.ac.uk/tools/fact/
[4]https://www.ifis.uni-luebeck.de/ moeller/racer/
[5]http://www.hermit-reasoner.com/
[6]https://www.w3.org/2001/sw/wiki/Pellet

```
1. SELECT ?reading
    WHERE {
        ?reading rdf:type MIoT:BloodPressureReading .
        ?reading MIoT:hasReadingValue ?value.
        FILTER (?value > 120)
    }
```

reading
BloodPressureReading1
BloodPressureReading2

Figure 5.2: The SPARQL Query Result.

The `BloodPressureReading` class has three instances. This query selects all instances of the BloodPressureReading class and their associated `hasReadingValue` property and applies a filter that checks if the reading value is greater than 120 as shown in Figure 5.2. The query returns a list of ?reading variables that correspond to blood pressure readings with values greater than 120.

```
2. SELECT ?reading
    WHERE {
   ?reading rdf:type MIoT:BloodPressureReading .
  ?reading MIoT:hasReadingValue ?value .
  FILTER (?value < 120)
    }
```

reading
BloodPressureReading3

Figure 5.3: The SPARQL Query Result.

This query selects all instances of the `BloodPressureReading` class and their associated `hasReadingValue` property and applies a filter that checks if the reading value is greater than 120. The query returns a list of ?reading variables that correspond to blood pressure readings with values lesser than 120 as shown in Figure 5.3.

```
3. SELECT ?value
    WHERE {
   ?bloodPressureReading1 rdf:type MIoT:BloodPressureReading .
   ?bloodPressureReading1 MIoT:hasReadingValue ?value .
   ?bloodPressureReading1 MIoT:hasPatient MIoT:John .
    }
```

Figure 5.4: The SPARQL Query Result.

This query selects all instances of the `BloodPressureReading` class and their associated `hasReadingValue`, and `hasPatient`. It applies a filter that targets readings for the specific patient `"John"` (?reading MIoT:hasPatient MIoT:John), as shown in Figure 5.4.

5.4 Conclusion

Remote Patient Monitoring involves IoMT to gathering patient data from a remote location and transmitting it to healthcare providers for analysis and treatment Knowledge organization systems are the best solutions to organize and arrange that information systematically. In this regard, MIoTOntology captures the semantics of the concepts and properties of the primary security aspects of IoT medical devices used in remote patient monitoring systems. SWRL rules are used to infer new facts and provide automated reasoning to enhance the security of IoMT networks used in Remote Patient Monitoring. Finally, SPARQL is used to extract the knowledge from the proposed ontology.

Chapter 6

Novel Knowledge Graph-Based Modeling for Vulnerability Detection in the Internet of Medical Things

This chapter presents the development of a semantic framework for vulnerability detection in Internet of Medical Things (IoMT) environments, along with a discussion of initial experimental results. The framework leverages semantic modeling to enhance data annotation and knowledge base creation, which supports the detection of vulnerabilities in medical IoT networks. Additionally, it generates a knowledge graph that stores Cyberthreat Intelligence (CTI) for these networks, offering a query mechanism to extract insights from the knowledge graph. This chapter was originally organized as an article. It is available online at `https://doi.org/10.1007/978-981-97-5937-8_26`; it has been adjusted here to meet the requirements of the thesis.

Abstract

In the evolving landscape of the Internet of Medical Things (IoMT) cybersecurity, traditional security measures often struggle with complex vulnerabilities, which are crucial due to the sensitive nature of patients' data. This chapter addresses this challenge and presents a comprehensive framework to enhance cybersecurity on IoMT. It proposes a novel MIoT ontology that integrates knowledge from diverse sources and employs RDF formalism for the semantic representation of medical devices and their related aspects. The framework also utilizes semantic modelling to enrich data annotation and knowledge base development, supporting the detection of vulnerabilities in medical IoT networks. Additionally, the framework generates a knowledge graph that stores Cyberthreat Intelligence (CTI) for medical IoT networks, enhancing vulnerability detection, while underscoring the significance of automated reasoning over aggregated knowledge.

6.1 Introduction

Smart technologies have reshaped how humans engage with their environment, offering unprecedented convenience, efficiency, and automation. From smart homes and cities to the expansive Internet of Things (IoT), these innovations aim to intelligently integrate digital and physical systems. Artificial

intelligence (AI) serves as a pioneering force in this technological evolution, profoundly impacting daily life. Its integration into the IoT has transformed interactions, enhancing service quality, efficiency, and overall productivity [237].

The Internet of Medical Things (IoMT) is a specific subset of IoT that is particularly transformative. It refers to the interconnected system of medical devices, software applications, health systems, and services that communicate with each other and with healthcare IT systems. The IoMT encompasses wearable devices such as fitness trackers, implanted devices such as heart monitors, and even hospital-based systems like surgical robots. The primary goal is to optimize patient care, enhance the quality and effectiveness of treatments, and increase the overall efficiency of healthcare delivery [192].

Since IoMT devices often deal with sensitive personal health information, they are potential targets for cyberattacks. The security concerns include data breaches, unauthorized access, and the potential for cybercriminals to manipulate medical devices, which could lead to life-threatening outcomes. For instance, in 2022, the U.S. Department of Health and Human Services reported 125 digital data breaches in healthcare nearly doubling from the previous year [44]. The upward trend persisted into early 2023, with 145 reported incidents in healthcare in the first quarter [45]. In March 2023, a report from HIPAA (The Health Insurance Portability and Accountability Act) highlighted a concerning pattern, with data breaches affecting over 4 million patients [46].

However, the integration of IoMT into healthcare systems brings forth significant security concerns. The rapid alteration in IoT applications in healthcare makes it challenging for cyber threats and vulnerabilities in knowledge organization systems. Very few systems can work in IoMT to model it in terms of interoperability and heterogeneity. In the case of medical devices, when any cyber-attack (i.e. ransomware or phishing) has occurred, the organization systems are not well developed to provide semantic knowledge to improve cyber resilience. This paper provides the basis for developing the knowledge graph-based modeling for vulnerability detection in IoMT setting, that is ultimately exploit attacks.

The rest of the paper is organized as follows. Section 2 discusses 'Related Work', followed by Section 3, which presents the Proposed Framework for Vulnerability Detection Utilizing Knowledge Graph-Based Modeling. Section IV provides a discussion. The conclusion and future work are presented in Section V.

6.2 Related Work

Several researchers work in IoMT settings and have proposed systems to enhance the security and privacy of patients by using different techniques such as ensemble learning, federated learning, blockchain machine learning and deep learning methods. Alsubaei et al. [238] proposed a Python-based recommendation tool utilizing an ontology, tailored to stakeholder-specific needs and scenario-based approaches. The tool's effectiveness was assessed through a vulnerability-based method and an expert-based method, involving the evaluation of 40 vulnerabilities from the NVD (National Vulnerability Dataset) dataset across 11 scenarios and incorporating recommendations from seven cybersecurity graduates. Their tool faces a few challenges, particularly in the complexity of IoMT environments,

ensuring adaptability to evolving IoMT solutions, and the potential difficulty for certain stakeholders, such as medical professionals and patients, to comprehend its recommendations. Additionally, it requires regular updates to address new IoMT solutions and security threats.

Recently, Khan et al., [162] proposed a Secure Ensemble Learning-Based Fog-Cloud Approach for Cyberattack Detection in IoMT, which addresses the security issues in IoMT networks caused by cyberattacks. One of the limitations of this research is that their approach was evaluated using a simulated environment, which may not accurately reflect the real-world performance of their approach. Additionally, the proposed approach may not be effective against new and unknown cyberattacks that have not been included in the training dataset. The research presented by [168] focuses on Federated Learning (FL), Artificial Intelligence (AI), and Explainable AI (XAI) in the context of intelligent healthcare. The primary aim is to address vulnerabilities and challenges in traditional healthcare systems that rely on centralized data sharing. In terms of challenges they faced, these include privacy issues, difficulties in aggregating user data from different sources, the potential failure of cloud systems in personalized settings, and the sensitivity of healthcare data.

The survey paper proposed by Jameel Almalki [170] focuses on analyzing current state-of-the-art blockchain technologies and their applications in IoT-based healthcare systems. It acknowledges the diversity in both the dimensions of existing blockchain approaches and the requirements of IoT-based healthcare applications. The main limitations identified include unresolved security issues such as hostile attacks and authentication challenges, ongoing issues with blockchain delay, and a lack of in-depth performance evaluation of the system. In another survey [183], researchers focus on exploring the use of modern technologies like the Internet of Things (IoT), 5G networks, artificial intelligence (AI), and big data analytics in enhancing healthcare solutions. It emphasizes the need for continued research to enhance the security aspects of modern healthcare systems, thereby addressing the prominent open-ended research challenges identified in the survey. Mahmood et al. [174] conducted a Systematic Literature Review focused on developing a security model for the IoMT. This involved analyzing major security models and conducting a meta-analysis to prioritize risks. The resulting model includes a Python-based interface for identifying and managing threats. However, the chapter recognizes the necessity for ongoing enhancements to the model, acknowledging the dynamic nature of security threats in the IoMT sector.

Sills et al., [185] aim to address security vulnerabilities in medical IoT devices by creating a comprehensive repository of Cyber Threat Intelligence (CTI), enabling the use of AI-based cyber defence systems. For this purpose, they proposed a system that generates CTI from sources such as manufacturer alerts, and ICS-CERT[1], and augments it with data from Wikidata and FDA[2]'s AccessGUDID. The combined information forms a Cybersecurity Knowledge Graph (CKG) that is further enhanced through graph embeddings. However, the lack of extensible big data resources for medical device vulnerabilities necessitates the need for knowledge augmentation, and the complexity of connecting diverse data sources in the CKG is one of the challenging tasks. Secondly, security risks associated with medical IoT devices, such as data breaches and device compromise, highlight the urgency of creating a reliable knowledge base to enhance cybersecurity measures in healthcare settings.

[1]Industrial Control Systems - Cyber Emergency Response Team

[2]Food and Drug Administration

Apart from it, the literature focused on the the key research areas in the field of IoMT to address security and privacy concerns [112; 167; 171]. Additionally, there's a growing focus on developing regulatory frameworks and standards [43; 100] to ensure IoMT devices meet minimum security requirements [101; 102]. However, they lack to provide semantic information for medical devices in terms of vulnerability detection. However, they lack the provision of semantic information for medical devices in terms of vulnerability detection. In contrast to existing techniques, this paper proposes a semantic framework that facilitates partial automation in improving the security posture of medical devices in remote patient monitoring (RPM). At the heart of this framework is a domain ontology, which captures the semantics of the concepts and properties of the main security aspects of IoT devices used in such systems. This is complemented by a security ruleset, complex queries, and a mechanism to enable automated reasoning over the aggregated knowledge.

6.3 A Proposed Framework for Vulnerability Detection Utilizing Knowledge Graph-Based Modeling

In this section, this study presents a proposed framework for vulnerability detection. This framework integrates the Internet of Medical Things ontology, a knowledge graph enriched with medical device data, and the incorporation of the National Vulnerability Database (NVD) CVE information via an API[3]. This methodology empowers the framework to offer predictions about vulnerabilities, thereby enhancing the security of remote patient monitoring systems. Figure 6.1 shows the working mechanism of the proposed approach. The details of each component including data storage and processing are provided in the following sections.

6.3.1 Knowledge Acquisition

The knowledge acquisition phase involves gathering comprehensive background knowledge from different sources such as literature, existing ontologies, standards, vocabularies, and manufacturers. This background knowledge is related to the fields of cybersecurity and IoMT, particularly remote patient monitoring. This process includes identifying commonly used medical devices in the IoMT settings, understanding potential vulnerabilities and attacks targeting these devices, and determining the relevant security requirements. Standards and vocabularies such as RDFs (Resource Description Frameworks) and schema.org are utilized to identify and represent the necessary data for developing the domain ontology IoMT. Data related to different types of IoT devices used in remote patient monitoring, potential cyberattacks, and their corresponding data types and functionality is collected. Extensive literature surveys are conducted to review existing ontologies in the cybersecurity field, such as the VulOntolog [239], which provides valuable concepts and properties that can be incorporated into the MIoT ontology for effective cybersecurity in remote patient monitoring systems.

[3]Application Programming Interface

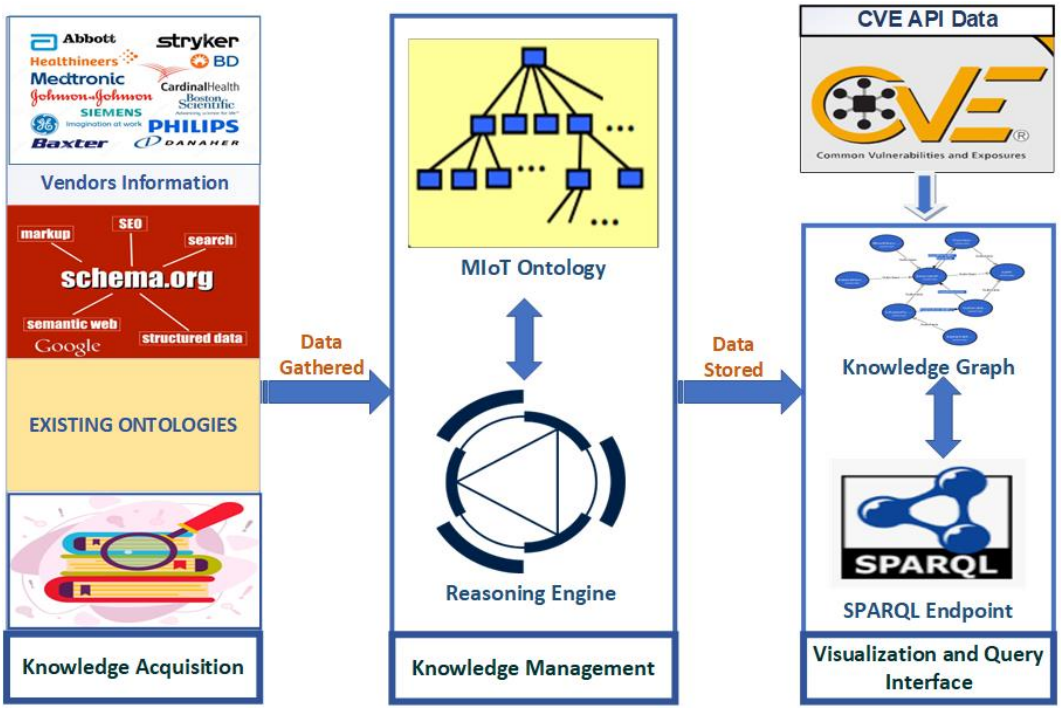

Figure 6.1: A Semantic Framework for Vulnerability Detection based on Knowledge Graph (Source of Images: Google).

6.3.2 Knowledge Management

Knowledge management plays a crucial role in the proposed framework, utilizing reasoning to infer new facts within the ontology. The framework employs rule-based reasoning, wherein rules are defined to describe logical conditions and to predict hidden relationships within the ontology. Knowledge management can be divided into two main parts, as follows:

6.3.2.1 MIoT Ontology

The development of an MIoT ontology for cybersecurity in remote patient monitoring systems starts with data acquisition, followed by defining relevant concepts and properties and annotating the data with semantic information. The MIoT ontology is central, incorporating healthcare expertise and literature to define the semantics of medical devices, vulnerabilities, and services. It uses RDF formalism for better representation and supports vulnerability detection in Medical IoT by enhancing data access, sharing, and automated reasoning. This ontology includes various concepts such as medical devices, vulnerabilities, users, etc., and their relationships, contributing significantly to IoMT security. The key purpose of MIoT ontology is:

a. ***Data Annotation:*** This involves annotating data with semantic information using the MIoT Ontology to enhance the semantics of the RPM domain. The ontology encompasses concepts related to vendors, products, medical devices, manufacturers, firmware, versions, vulnerabilities, exploits, and affected components of medical devices, including operating system (OS), hardware, and applications.

b. ***Knowledge Base Development:*** This process utilizes concepts, instances, and their relationships derived from knowledge acquisition. The knowledge base comprises a collection of data points (instances) and the categories or ideas they represent (concepts), all interconnected through relationships. This structure is vital for organizing and interpreting complex, diverse information in a meaningful way, particularly in domains like IoMT.

6.3.2.2 Reasoning Engine

Extending the domain ontology with rules and complex queries enables reasoning capabilities that go beyond simple data retrieval. It can identify potential vulnerabilities, assess the impact of vulnerabilities, and recommend mitigation strategies based on the knowledge encoded within the ontology and the rules.

For instance, this framework may employ a rule that associates a particular firmware version with a known vulnerability based on the NVD dataset. "This rule allows to identify all devices with the same firmware, version as potentially vulnerable". By utilizing complex queries, it can further analyze the network topology, device configurations, and other relevant factors to assess the potential impact of these vulnerabilities on the overall system.

The semantic framework facilitates automated reasoning over aggregated data from various sources, such as the MIoT ontology, CVE information, and any other external source. In rule-based reasoning, rules are used as a fundamental mechanism to draw conclusions or make decisions. Rule-based systems evaluate data or facts against these rules to infer new information or make decisions.

For example:

```
X= CardiacRhythmManagement is a MedicalSensor
Y= MedicalSensor is a subClassOf MedicalIoTDevice
Z= CardiacRhythmManagement is a MedicalIoTDevice
```

In the rule-based systems, this transitive property shows If X=Y and Y=Z then X=Z.

In rule-based reasoning, software agents efficiently apply predefined rules to data, identifying relevant patterns and executing corresponding actions or conclusions. Their automated processing capabilities are essential for decision-making or in environments where human expertise needs to be emulated or augmented. For example, a rule state that:

If a medical device firmware version x from the vendor y is known to have a specific vulnerability (based on historical data or NVD CVE information), then all devices with the same firmware version are considered vulnerable". This rule is represented in SWRL (Semantic Web Rule Language) and DL (Description Logic) syntax as follows:

SWRL Rule

```
Product(?product) ∧ hasFirmware(?product, ?firmware) ∧ hasVendor
(?product, ?vendor) ∧ hasVulnerability(?firmware, true) ∧ Product
(?otherProduct) ∧ hasFirmware(?otherProduct, ?firmware) ∧ hasVendor
(?otherProduct, ?vendor) ∧ DifferentFrom(?product, ?otherProduct)
                    → is vulnerable(?product, true)
```

DL Axioms

$$\forall x.\,\text{Product}(x) \land \exists f.\,\text{hasFirmware}(x, f) \land \exists v.\,\text{hasVendor}(x, v)$$
$$\land \exists w.\,\text{hasVulnerability}(f, w) \land w = \text{true} \rightarrow \text{isVulnerable}(x, \text{true})$$

This axiom shows that, if a product has firmware with a vulnerability, then the product is vulnerable.

$$\forall x.\forall y.\forall f.\forall v.\,\text{Product}(x) \land \text{Product}(y) \land \text{hasFirmware}(x, f) \land \text{hasFirmware}(y, f)$$
$$\land \text{hasVendor}(x, v) \land \text{hasVendor}(y, v) \land x \neq y \rightarrow \text{isVulnerable}(x, \text{true})$$
$$\land \text{isVulnerable}(y, \text{true})$$

This axiom shows that, if two different products have the same firmware and the same vendor, then both products are vulnerable.

6.3.3 Visualization and Query Interface

The ontology data is stored in a knowledge graph, which also includes the data source NVD (National Vulnerability Database) with its Common Vulnerabilities and Exposures (CVE) data to display vulnerabilities associated with medical devices in the ontology. The knowledge graph provides visualization capabilities, allowing users to view the relationships and connections within the graph. Additionally, it offers a SPARQL endpoint that enables users to query the graph and assess the effectiveness of the framework. It consists of three parts:

6.3.3.1 MIoT Knowledge Graph

A knowledge graph is a graph-based data structure that represents knowledge through entities, relationships, and attributes. It offers a flexible way to organize, query, and enhance understanding of data. In this framework, a knowledge graph is proposed, based on the developed MIoT ontology. The initial version of MIoT Ontology is published in [135]. Utilizing semantic modelling and the NVD dataset, this cybersecurity knowledge graph is populated with Cyber Threat Intelligence (CTI) about vulnerabilities in medical devices within IoT networks.

In this research, the OntoText GraphDB [4] tool to generate the IoMT knowledge Graph that stores the CTI of IoT networks in medical devices. This facilitates the detection of vulnerabilities, thereby strengthening the protection of patient data. Figure 6.2 illustrates the domain-range graph for the IoMT

[4]https://www.ontotext.com/

knowledge graph. Where it showcases the various concepts (i.e., Vulnerability, Vendor, Services etc.,) and their relationships (i.e., hasVendor, byUsingService, usingDevice etc.,) with the concept Product.

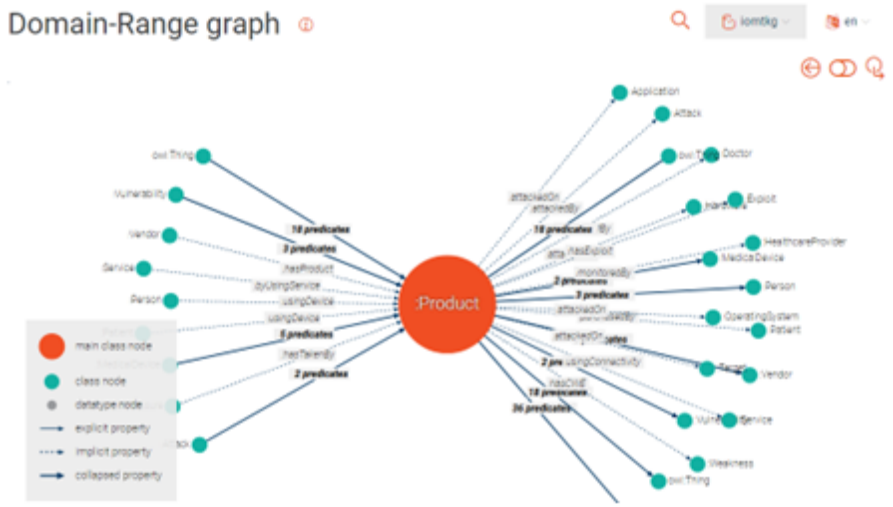

Figure 6.2: The Domain-Range graph for the concept Product.

6.3.3.2 Integration with Industry Standards

The National Vulnerability Database (NVD) is a U.S. government repository that provides standards-based vulnerability management data. This includes details on security-related software flaws, misconfigurations, product names, and impact metrics. The NVD is essential for the IT security community, offering a comprehensive database to evaluate and manage cybersecurity risks linked to known vulnerabilities in software products and systems. It serves as a crucial tool for cybersecurity professionals to identify and address vulnerabilities in network and software environments.

This semantic framework utilizes the National Vulnerability Database (NVD) dataset for a detailed analysis of vulnerabilities in medical IoT networks. The NVD offers a standardized collection of known vulnerabilities and exploits in such settings. The integration of this dataset allows to identify specific vulnerabilities in these systems. To seamlessly incorporate the NVD by utilizing an API to access up-to-date information on Common Vulnerabilities and Exposures (CVE) and the Common Vulnerability Scoring System (CVSS). The NVD API allows users to access NVD data and allowing the integration of this information into the proposed framework programmatically. The API can be used to automatically update security systems with the latest vulnerability information, including security checklists, security-related software flaws, product names, and impact metrics. This ensures that the proposed framework is continuously updated with the latest data from the NVD, providing ongoing protection against new threats in remote patient monitoring IoT networks.

6.3.3.3 Access to the SPARQL Endpoint

The SPARQL endpoint enables access to the knowledge graph's interface, allowing users, including patients, doctors, and healthcare providers, to visualize, query, and update data. For example:

```
SELECT ?Product ?Condition ?y ?p ?e
WHERE {
    ?Product a base:MedicalSensor .
    ?Product IoMT:monitor ?Condition .
    ?x base:vulnerabilityID ?y.
    ?x base:hasPublished ?p.
    ?x base:hasExploit ?e.
    filter (?y = "CVE-2023-1729") .
}
```

The above mentioned query retrieves all those products whose CVE ID is CVE-2023-1729, along with other relevant information such as functionality provided by the product, its published date, and exploit.

```
SELECT ?Product ?Condition ?y ?p ?w
WHERE {
    ?Product a base:MedicalSensor .
    ?Product IoMT:monitor ?Condition .
    ?x base:vulnerabilityID ?y.
    ?x base:hasPublished ?p.
}
```

This query retrieves those products with the name of medicalSensor along with their functionality, VulnerabilityID and when it was published.

6.4 Discussion

In the rapidly evolving domains of IoT and cybersecurity for IoMT, existing security measures often fall short, especially in handling complex vulnerabilities with significant semantic implications. These shortcomings are critical due to the sensitive nature of patient data, underscoring the need for improved, automated security solutions on the Internet of Medical Things (IoMT). Several ontologies addressing various aspects of this domain have been published in the realm of IoT, IoMT and cybersecurity [63; 238; 239; 240] among others. However, the proposed research introduces a comprehensive ontology that represents medical devices, users, vendors, vulnerabilities, and more within the RPM cybersecurity context. This ontology aims to capture the domain's semantics and establish meaningful relationships between entities.

Additionally, a significant deficiency of traditional security measures is their lack of automation. This issue becomes particularly problematic in the rapidly changing cybersecurity landscape, where new vulnerabilities constantly emerge. Without automated systems to quickly identify and respond to these threats, there's a delay between the emergence of a vulnerability and its mitigation. This delay allows attackers to exploit these weaknesses before users or administrators become aware of them. This situation underscores the need for more dynamic, intelligent, and automated security solutions

in the IoMT field, capable of proactively addressing threats in real-time to protect sensitive patient data. Existing knowledge graphs populate NVD CVE information from JSON/XML files of the NVD dataset. This framework stands out by using an API to access and incorporate data, ensuring regular updates and the ability to address emerging vulnerabilities.

6.5 Conclusion and Future Work

In this chapter, a semantic framework is proposed that combines the Medical Internet of Things Things (MIoT) ontology with a knowledge graph enriched by medical device data and integrates CVE information from the National Vulnerability Database (NVD) via an API. The proposed approach enables the system to detect vulnerabilities, thereby improving the security of remote patient monitoring systems. The knowledge graph concisely presents Cyber Threat Intelligence (CTI) information, offering advantages over traditional relational databases. In addition, it demonstrates the importance of automated reasoning over aggregated knowledge by presenting example rules. Future work will focus on employing a reasoning engine to perform automated reasoning, aimed at identifying vulnerabilities. This will allow the framework to showcase advanced notifications about vulnerabilities and potential attacks.

Chapter 7

Implementation, Testing and Validation

The previous chapter presented a few results from the development of the semantic framework. The initial results were derived from the MIoT ontology, and based on that information, a knowledge graph (KG) was created and queried to test the semantic framework. However, the most important part of this research, automated reasoning, was discussed with a few examples. The automated reasoning was not performed on existing knowledge by a rule-based engine.

This chapter presents the implementation of the entire semantic framework, comprising two core components. The first part includes a semantic model that implements the MIoT ontology, generates the rulesets, and performs reasoning using an inference engine, that shows the hidden relationships and infers the new facts. The second part consists of a knowledge graph that stores data from the semantic model and integrates it with the NVD database via an API for visualization. This knowledge graph can be accessed through SPARQL queries to assess vulnerabilities in the system.

The purpose of this chapter is to demonstrate the implementation of the semantic framework presented in this thesis. This is important for several reasons. Firstly, it demonstrates verification and reproducibility, allowing other researchers and reviewers to verify the applicability of the framework and confirm that it can be applied as claimed. Secondly, the ability to reproduce its applicability enables other researchers to achieve similar results and build upon this work in future iterations of the framework. A third benefit of demonstrating the implementation is to show how the theoretical concepts have been translated into practical applications. It also assists in revealing potential errors or assumptions that are built into the framework, which might not be evident from a high-level description.

By showing the implementation, testing, and validation, this chapter highlights the educational value of the framework and serves as a valuable learning tool for researchers and practitioners who want to understand its practical aspects. At the same time, it demonstrates the technical proficiency and ability to apply theoretical knowledge to real-world problems in the context of the Internet of Medical Things (IoMTs). This chapter showcases the novel techniques involved in the application of this framework, drawing upon the combinational novelty of the ontology and rulesets used with automated reasoning. It emphasizes the framework's applicability to solving real-world challenges, thereby demonstrating the practical relevance and impact of the work. This chapter shows that the work is thorough, transparent, and valuable.

Additionally, the semantic model is evaluated using a standardized knowledge engineering method-

ology and large language models such as generative AI models to validate the case study provided in *Chapter 4*. In this regard, a research article [241] is accepted in International Conference `http://kes2024.kesinternational.org/`. Finally, the semantic framework is validated against an existing framework that utilized IoMT components to identify security issues and provide a recommendation tool for vulnerability detection.

7.1 A Semantic Framework for Vulnerability Detection in Remote Patient Monitoring

The primary objective of this research is to develop a semantic framework that partially automates the enhancement of security in IoT networks used for remote patient monitoring (RPM). The MIoT semantic framework comprises two core components, as shown in Figure 7.44.

The first component is a semantic model that includes the MIoT ontology and an inference engine. The semantic model is created by incorporating background knowledge, entity relationships, annotations, and individuals. The knowledge base consists of facts (RDF triples) and rules. The MIoT ontology is implemented by generating a set of rules that perform automated reasoning to identify hidden vulnerabilities and anomalies in the system. The rule management module is essential for ensuring that the rules within the inference engine are correctly defined, efficiently managed, and effectively executed, enabling various reasoning techniques to work together in drawing conclusions and making decisions in rule-based systems. The RDF triples from the semantic model, along with the inferred knowledge, populate the knowledge base.

The second component is a visualization and query interface. This component features a knowledge graph designed to store cyber threat intelligence (CTI) for semantic representation, visualization, and data integration. Knowledge graph Set up the fundamental structure of the knowledge graph in the form of nodes and edges and incorporate Cyberthreat Intelligence (CTI) data into the graph. The RDF triples, after reasoning, are exported from the knowledge base to the MIoT Knowledge Graph. This graph now contains enriched and structured data that can be queried and analyzed. CVE and CVSS information from the NVD database is fetched via an API. This live data is integrated into the MIoT Knowledge Graph, ensuring the graph is updated with the latest vulnerability information. Finally, visualization tools display the data interactively, enhancing comprehension and facilitating decision-making.

The knowledge graph supports various queries through a SPARQL endpoint. Users can run specific queries to extract relevant information. SPARQL queries are employed to query semantic data and extract insights from the knowledge graph. The MIoT Knowledge Graph is continuously updated and enriched with semantic data and real-time vulnerability information, providing a robust platform for querying, analyzing, and visualizing the data. The detailed working mechanism of the MIoT semantic framework is discussed in the rest of the chapter.

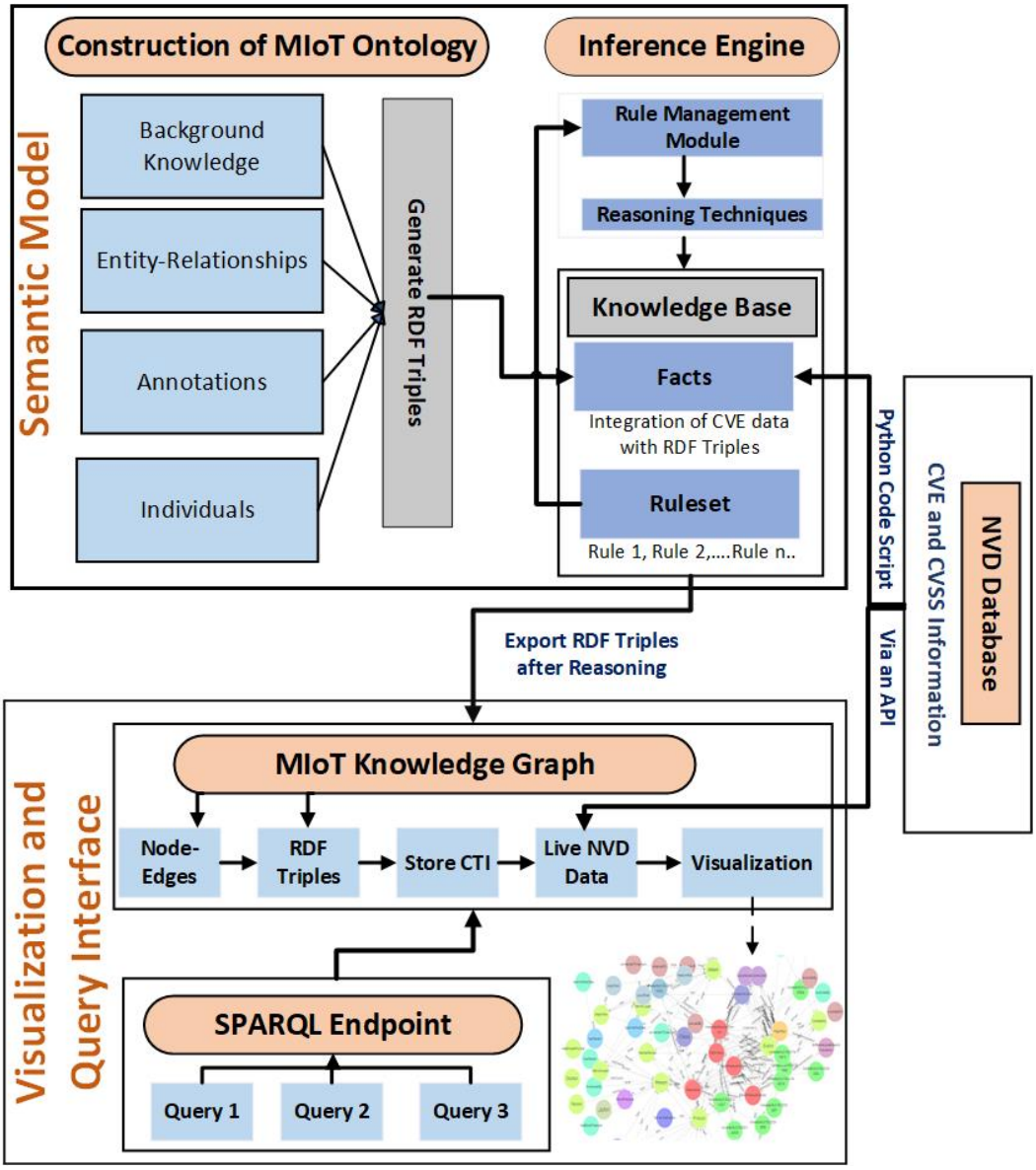

Figure 7.1: A Semantic Framework for Vulnerability Detection in Remote Patient Monitoring .

7.1.1 Semantic Modelling

Semantic modelling plays a crucial role in IoMT, addressing interoperability and heterogeneity to enable data processing and decision-making [104]. Semantic models represent medical information and knowledge in a structured and machine-readable format, facilitating the sharing and integration of information among various systems such as healthcare and cybersecurity.

Ontology is one of the key components of semantic modelling, encompassing various types of information beneficial to the represented domain. This includes concepts, along with their attributes and potential representations, relationships among concepts (involving subclasses, synonyms, and constants), axioms, functions associated with these concepts, and instances of these concepts along with their interrelations and the axioms governing them. The initial three categories constitute the schema information (also denoted as the conceptual model or meta-knowledge), while the last category pertains to instance knowledge [242].

However, this chapter only focuses on semantic modeling in terms of ontology implementation,

rule set generation, and reasoning mechanisms. The MIoT ontology schema and its conceptual model are presented in Chapter 4, where the entire process of defining concepts, properties, and their attributes has already been covered.

7.1.1.1 Implementation of MIoT Ontology

For effective ontology development, Classes, Objects, Properties, and Relations must be accurately configured in an RDF (Resource Description Framework), OWL (Web Ontology Language), or XML (Extensible Markup Language) format. Initially, the core schema for the MIoT ontology was designed and implemented in the semantic web standard RDF[1]. RDF has various formats such as RDF/XML, N-Triples, TriG, Turtle, among others [243].

The MIoT ontology is developed in Turtle format[2], where triples are generated in the form of Subject-Predicate-Object (S→P→O). The example of MIoT ontology in RDF Turtle format is provided online[3]. The prefixes used in MIoT ontology are provided in Table 7.1 .

Table 7.1: Prefix Definitions

Prefix	**IRI**
`@prefix :`	`<http://purl.org/ontology/MIoT/>`
`@prefix dc:`	`<http://purl.org/dc/terms/>`
`@prefix owl:`	`<http://www.w3.org/2002/07/owl#>`
`@prefix rdf:`	`<http://www.w3.org/1999/02/22-rdf-syntax-ns#>`
`@prefix xsd:`	`<http://www.w3.org/2001/XMLSchema#>`
`@prefix MIoT:`	`<http://purl.org/ontology/MIoT/>`
`@prefix rdfs:`	`<http://www.w3.org/2000/01/rdf-schema#>`
`@prefix schema:`	`<https://schema.org/>`
`@base`	`<http://purl.org/ontology/MIoT/>`

As the RDF Turtle file is a stand-alone file, this study needs to import the instances from the NVD database. For this purpose, the NVD data is imported into the MIoT ontology through a Python code **(details provided in Section 7.1.1.2)** in this chapter to generate an OWL file as the resultant ontology. The OWL ontology is imported into the Protégé desktop application. This study utilizes the Protégé Desktop application with the current version v.5.6.3. The first version, v.5.5.0, was released in March 2019[4].

The prototype of the MIoT ontology has been published[5], detailing its development and implementation. This publication discusses few examples of rule set generation for detecting vulnerabilities and anomalies resulting from cyber threats in medical devices and performs reasoning on them. In this chapter, the MIoT ontology is improved and adjusted according to requirements, incorporating CVE (Common Vulnerabilities and Exposures) information into the ontology. The high-level concepts of the MIoT ontology are discussed here in detail. The yellow dots in the figures show the concepts,

[1] https://www.w3.org/RDF/
[2] https://www.w3.org/TR/turtle/
[3] https://archive.org/details/mio-tontology-turtle-format
[4] https://protege.stanford.edu/
[5] `https://doi.org/10.1016/j.procs.2023.10.342`

the purple dots show the individuals, and the arrows show the relationships between concepts and individuals.

(a) Product

A product refers to any device, instrument, machine, implant, or component that is intended for use in the diagnosis, treatment, monitoring, or prevention of disease or other medical conditions. In MIoT Ontology, a `Product` is a concept or superclass of `MedicalDevice`. Figure 7.2 shows the relationship of the concept `Product` with other concepts such as `Vendor`, `MedicalDevice`, `Attack`, `Vulnerability` etc., and with individuals such as InfusionPump, ImplatableCardiacMonitor etc.

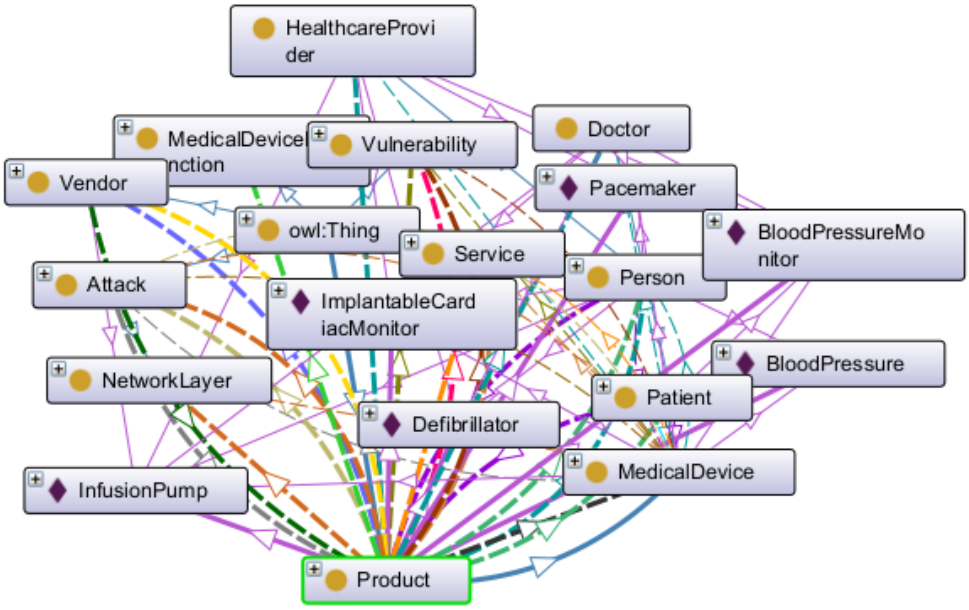

Figure 7.2: The relationship of `Concept_Product` with its subClasses and individuals.

(b) Medical Device

A very important concept in MIoT ontology is a medical device, which can be any instrument, apparatus, implement, machine, implant, or reagent for in vitro use, intended by the manufacturer to be used, alone or in combination. A medical device is used by human beings for one or more of the specific medical purposes such as diagnosis, prevention, monitoring, treatment, or alleviation of disease. The concept of Product and Medical device look similar in some places however this study put the MedicalDevice concept as a `subClass:Product` relationship. Because, in the literature, the vendors produce products as the main entity with multiple medical devices. Figure 7.3 shows the `MedicalDevice` concept with its related subClasses `Actuator`, `MedicalSensor` and `SensorAndActuator`, and others along with individuals such as Pacemaker, Glucometer etc.

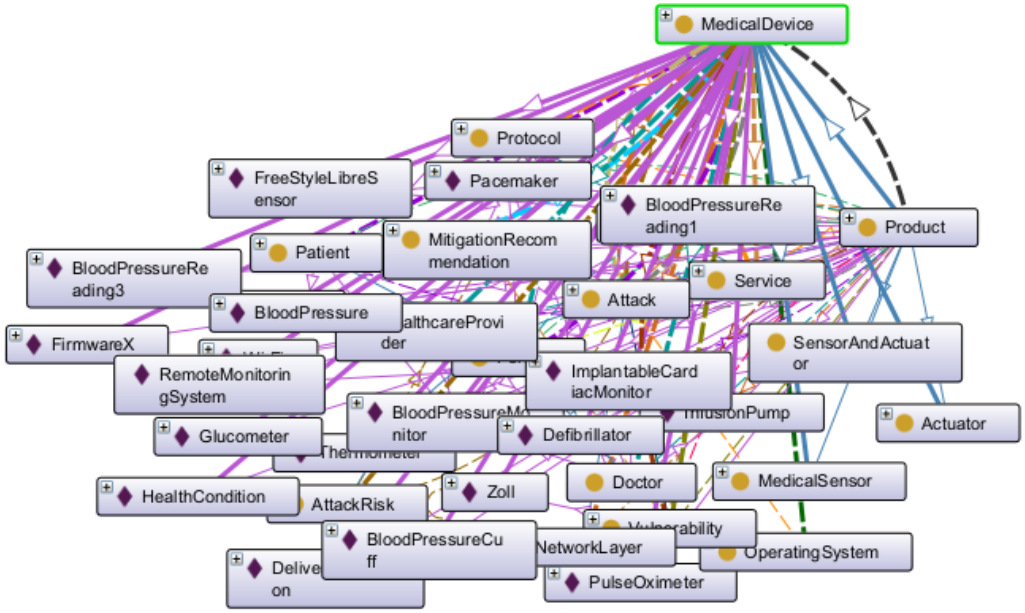

Figure 7.3: The relationship of `Concept_MedicalDevice` with its subClasses and individuals.

(c) Vulnerability

A vulnerability refers to a weakness or flaw in a system, network, or application that could be exploited by a threat actor to compromise the integrity, availability, or confidentiality of data or system resources. In the MIoT ontology, CVE instances are assigned to the Vulnerability concept. Figure 7.4 illustrates VulnerabilityCVE instances along with properties such as hasIntegrityImpact, hasConfidentialityImpact, and hasAvailabilityImpact, fulfilling the CIA (Confidentiality, Integrity, Availability) requirements within the domain of cybersecurity.

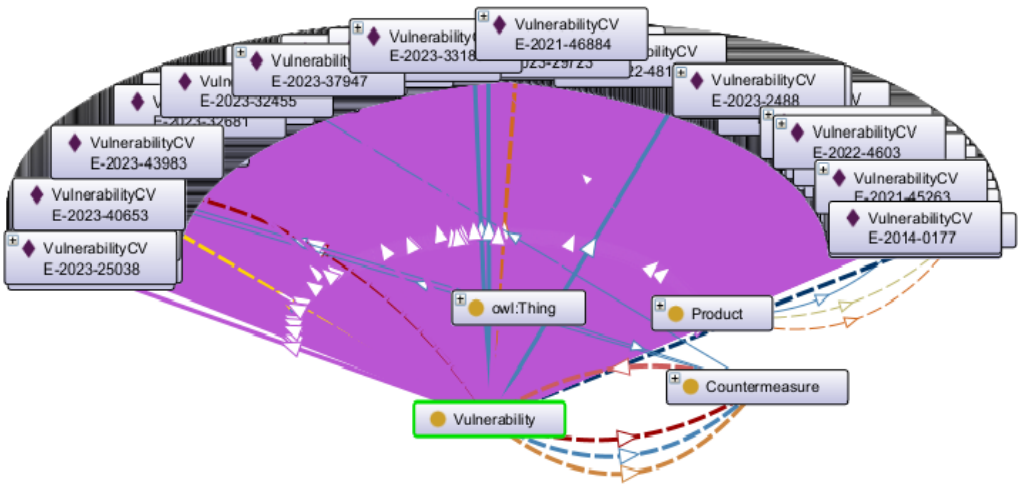

Figure 7.4: The `Concept_Vulnerability` with its subClasses, relationships and individuals.

(d) Service

The word ”service” is very broad. In terms of IoMT security, a ”service” refers to a digital function or capability offered by a device, system, or platform within the Internet of Medical

Things (IoMT) ecosystem. These services could include standards, technologies, and protocols responsible for data transmission, data storage, device management, access control, or any other functionality aimed at ensuring the security, integrity, and availability of medical devices and patient data within the IoMT network, as shown in the Figure 7.5

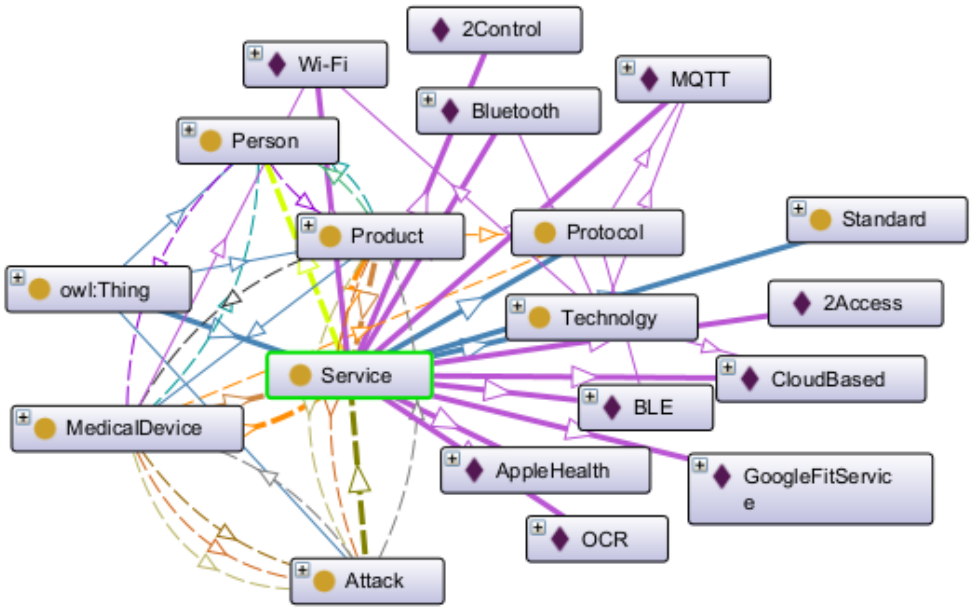

Figure 7.5: The `Concept_Service` with its subClasses, relationships and individuals.

(e) Person

In the context of IoMT Security, a person is any Patient, Doctor or Healthcare Provider. A person is connected to a medical device and facilitated by medical device functions. For example, a patient using a medical device, an Infusion Pump whose function is to deliver medication to a Patient. Figure 7.6 shows the relationship of Concept Person with its neighbours.

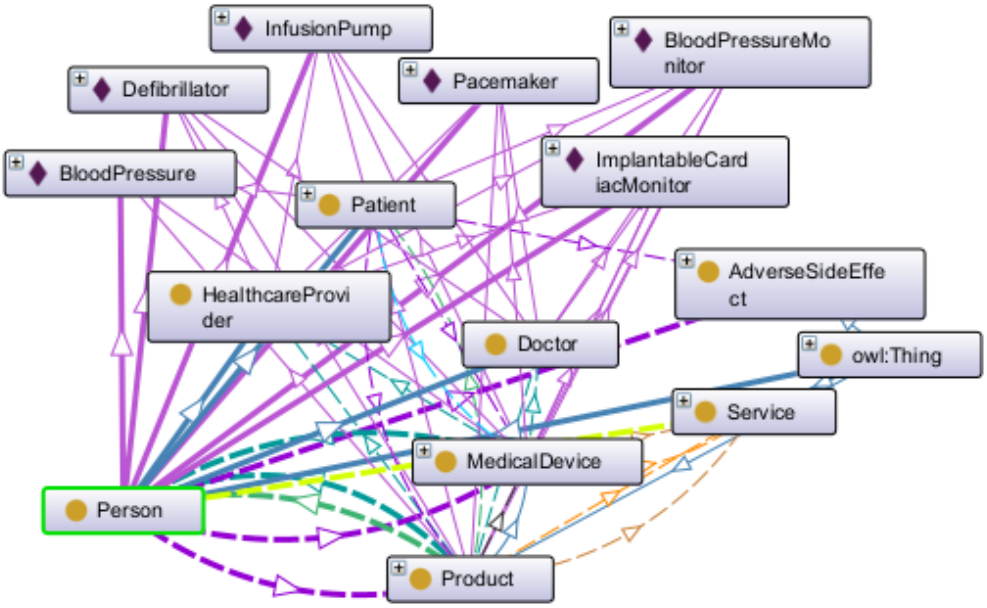

Figure 7.6: The relationship of `Concept_Person` with subClasses and individuals.

(f) Vendor

In the context of medical products, a ”vendor” as shown in Figure 7.7 refers to a company or organization that manufactures, distributes, or sells medical devices, equipment, supplies, or pharmaceuticals. Vendors play a crucial role in the healthcare industry by providing healthcare providers with access to essential products and technologies needed to deliver patient care.

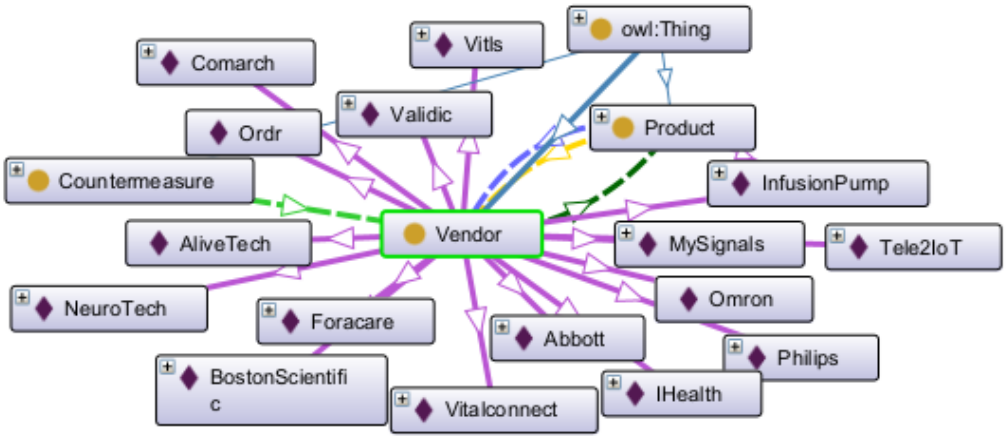

Figure 7.7: The relathionship of `Concept_Vendor` with other classes and individuals.

(g) Attack

In cybersecurity, an ”attack” refers to any malicious attempt to compromise the confidentiality, integrity, or availability of information or information systems. An Attacker employs various techniques, such as exploiting vulnerabilities in software or systems, social engineering, or using malware, to gain unauthorized access, steal sensitive data, disrupt operations, or cause other types of harm. Figure 7.8 shows the relationship of concept `Attack` with `Vulnerability`, `MedicalDevices`, `AttackRisk` etc.

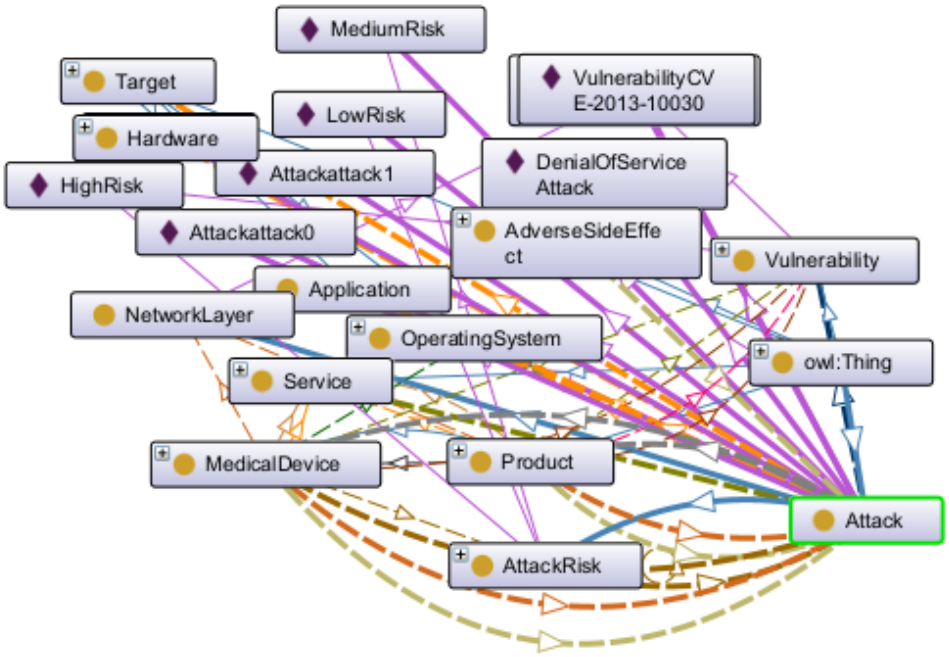

Figure 7.8: The relationship of `Concept_Attack` with its subClasses and individuals.

(h) AdverseSideEffect

An ”adverse side effect” is a harmful consequence resulting from a particular action, treatment, or intervention. In the context of healthcare, adverse side effects typically refer to unintended and undesirable effects of a medication, medical procedure, or treatment. These effects can range from mild discomfort to severe complications and can impact a patient’s health and well-being, potentially leading to life-threatening situations as shown in Figure 7.9

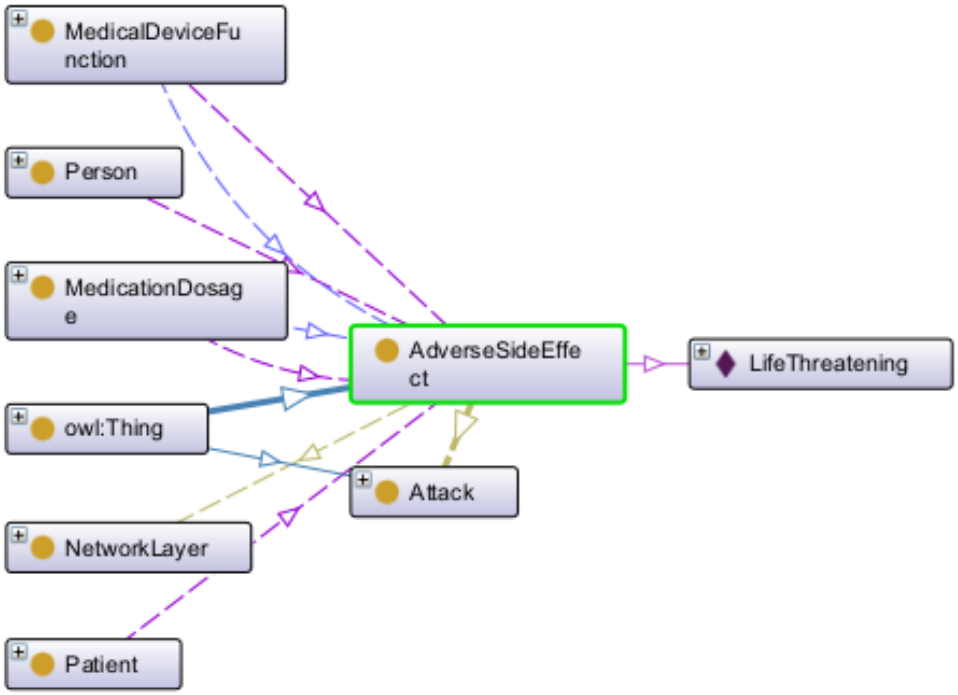

Figure 7.9: The `Concept_AdverseSideEffect` with its neighbour concept and individuals.

(i) Countermeasure

A ”countermeasure” is an action taken to prevent, mitigate, or neutralize a threat or potential risk to a system, organization, or individual. In cybersecurity, countermeasures are implemented to protect against attacks, vulnerabilities, and security breaches. These measures can include security protocols, software patches and other defensive strategies aimed at enhancing the security posture of a system or network. Figure 7.10 describes the effect of vulnerability and countermeasures are taken. Furthermore, to provide a robust and comprehensive security strategy, effective practices involve not only responding to threats as they occur (countermeasures) but also proactively reducing risks and preparing for potential vulnerabilities (mitigation). In this regard, the MIoT ontology models ”Countermeasure” as the main class, with ”Mitigation” and ”MitigationRecommendation” as its subclasses.

(j) Exploit

In cybersecurity, an ”exploit” refers to a piece of software, a sequence of commands, or a technique used by attackers to take advantage of a vulnerability or weakness in a system, application,

or network. Exploits are used to gain unauthorized access to a system, execute malicious code, steal data, or disrupt normal operations. Exploits can target software vulnerabilities, misconfigurations, or weaknesses in user behaviour to achieve their malicious objectives. The relationship of exploit with attacker and vulnerability and its individuals are illustrated in Figure 7.11

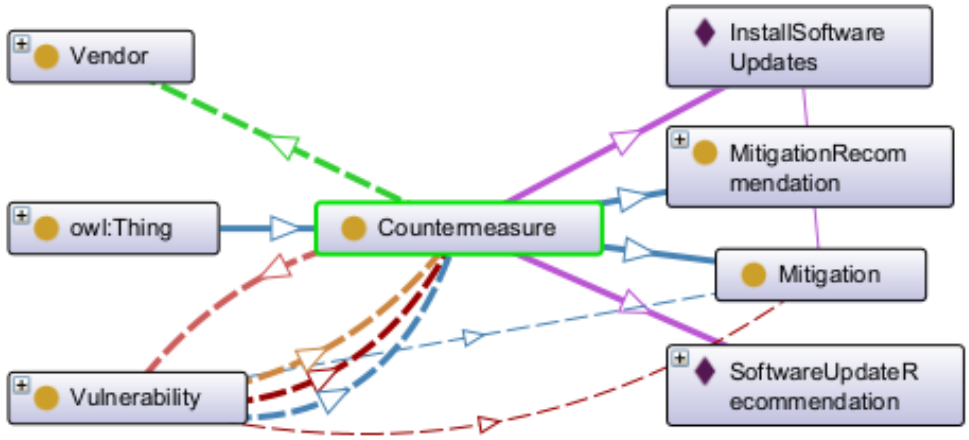

Figure 7.10: The relationship of `Concept_Countermeasure` with its subClasses and individuals.

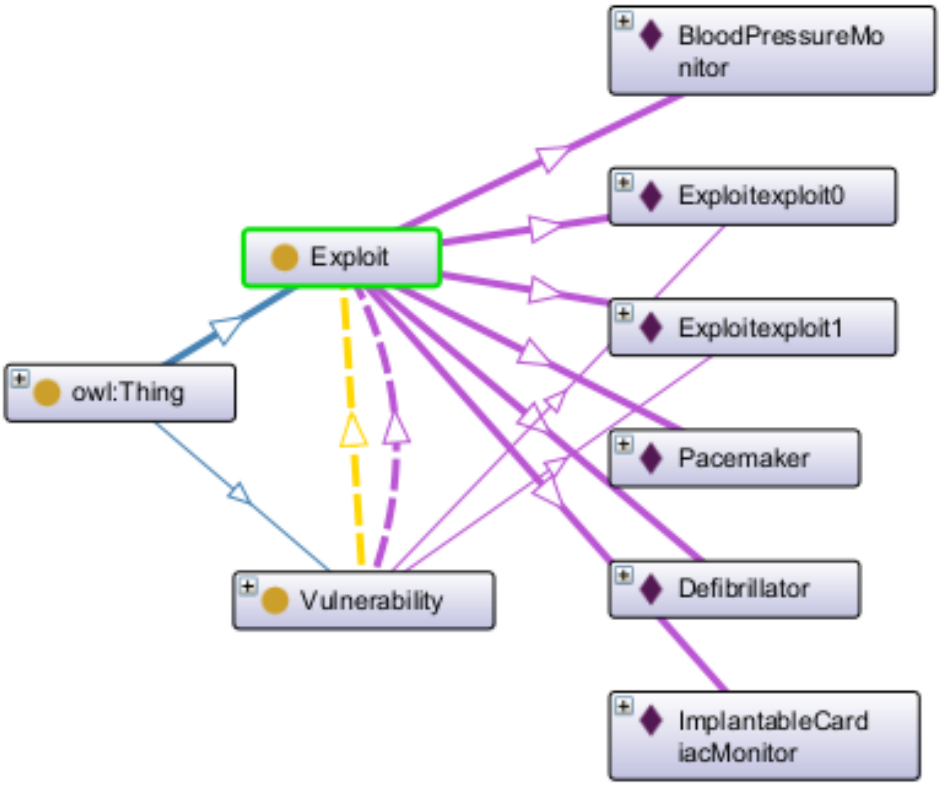

Figure 7.11: The `Concept_Exploit` with neighbour concepts, relationships and individuals.

(k) MedicalDeviceFunction

A ”medical device function” refers to the specific capability or operation performed by a medical device to diagnose, treat, monitor, or prevent diseases or medical conditions. These functions

can vary widely depending on the type of medical device and its intended use. Examples of medical device functions include measuring vital signs, delivering medication, providing imaging or diagnostic services, monitoring patient activity, and facilitating communication between healthcare providers and patients. Figure 7.12 shows the various medical functions in terms of individuals and their relationship with other concepts.

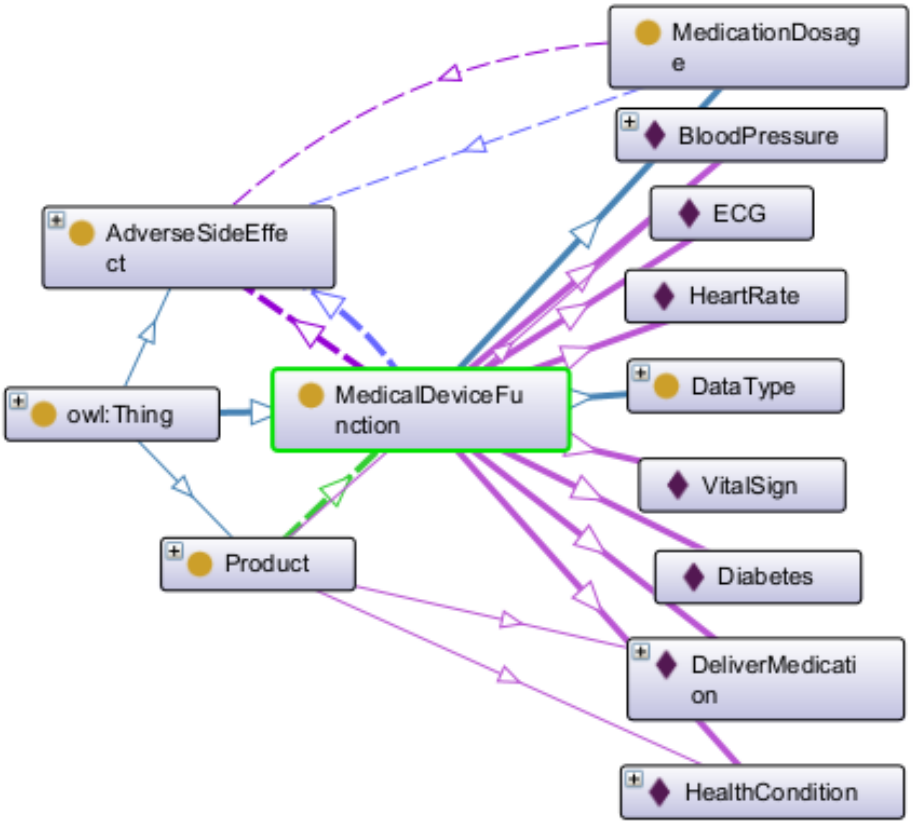

Figure 7.12: The `Concept_MedicalDeviceFunction` with neighbour concepts, relationships and individuals.

(l) Target

In the context of cybersecurity, a ”target” refers to an entity or system that is the focus of an attack or a potential attack. This could be a specific individual, organization, network, system, application, or device that an attacker aims to compromise, disrupt, or gain unauthorized access to. In MIoT ontology the concept Target has three subClasses Opertaing System, Hardware and Application as shown in Figure 7.13.

The MIoT ontology is designed to define concepts at multiple levels of granularity, covering three distinct tiers. At Level 1, foundational or high-level concepts such as Product, Vulnerability, Exploit, Person, and Service are established (as shown above). Level 2 extends this framework to include domain-specific entities, introducing terms like Patient, Healthcare Provider, and Technology. Finally, Level 3 refines the ontology with specialized subclasses such as Medical Sensor and Actuator. Figure 7.46 provides a detailed illustration of the hierarchical structure of MIoT ontology and its subclasses across these three levels. It is important to note that lower-level occurrences are facilitated through rule-based reasoning, which includes security elements will be discussed in *Section 7.1.1.3*.

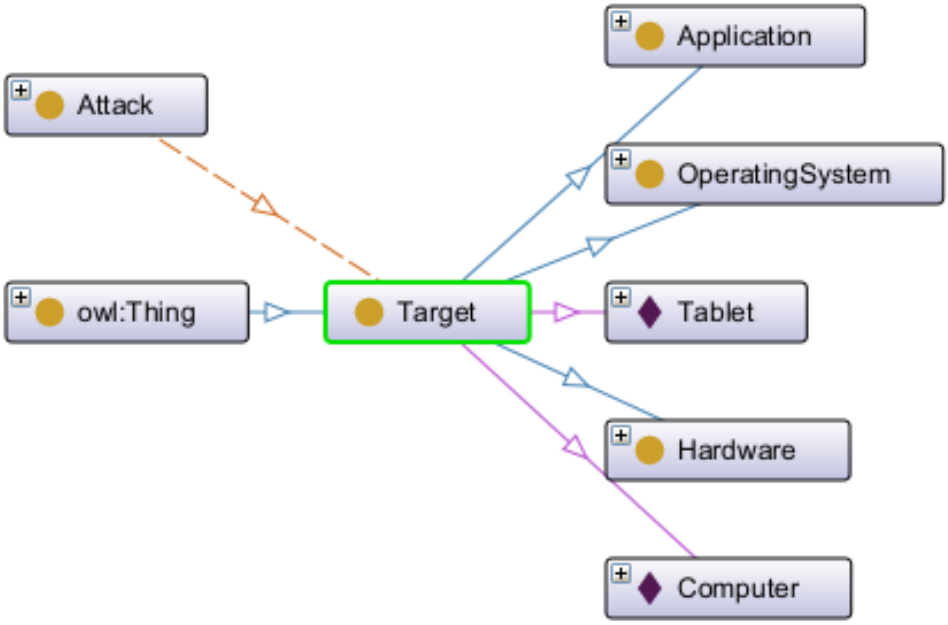

Figure 7.13: The `Concept_Target` with its subClasses, relationships and individuals.

7.1.1.2 Integration with NVD Database

One aspect of the semantic framework is its integration with the National Vulnerability Database (NVD). Operated by the National Institute of Standards and Technology (NIST), the NVD acts as a comprehensive repository for vulnerability data, drawing from various sources including CVE, vendor advisories, and security research organizations. The NVD aggregates this information and enriches it with additional metadata such as severity scores and impact assessments.

This integration aims to enhance decision-making by providing a structured and detailed view of vulnerabilities and their potential impacts. This study focuses on enumerations, severity scores, and impact assessments within the NVD. Enumerations create standardized identifiers for referencing shared data objects through the Common Vulnerabilities and Exposures (CVE) system. CVE serves as a repository of publicly documented information security vulnerabilities and exposures. These common identifiers within CVE facilitate the exchange of data among security products and provide a foundational point of reference for evaluating and tracking vulnerabilities across different platforms and organizations, overseen by MITRE.

Furthermore, the severity scores and impact assessments are typically components of the Common Vulnerability Scoring System (CVSS). CVSS provides a standardized method for assessing and communicating the severity of security vulnerabilities based on metrics such as ”Low,” ”Medium,” and ”High”. According to the Medical Device Regulation (Regulation (EU) 2017/745), the risk class of medical devices with vulnerability severity determined by the CVSS provides valuable insight into the current risks within National Health Systems [244].

The MIoT ontology represents the domain of medical devices and their related concepts and can be extended to include information about vulnerabilities. This extension would incorporate CVE data directly into the MIoT ontology, defining concepts, properties, and relationships related to CVE entries for medical devices. This approach allows for a more tightly integrated representation of CVE data

within the domain ontology.

To achieve this, this study integrates CVE data with the semantic framework in two ways: firstly, through Python code with the MIoT ontology, and secondly, through the NVD API with a knowledge graph. Both methods are discussed below.

(a) ***Method 1:*** **Integrating CVE data with Ontology (via Python code)**

The NVD CVE data is obtained from the NVD website in the form of a JSON file. The MIoT ontology, saved in OWL format with Protégé, contains the `hasCVE` property of the **??** concept, which has been mapped to CVE entries from the NVD dataset. With the help of Python code, the instances from the NVD database and the data from the MIoT ontology are integrated to create a new ontology. The Python code is available in Appendix C, and the pseudocode for the Python code is presented in this chapter as an Algorithm 2.

Algorithm 2 Pseudocode for Python Program NVD JSON File

Step 1: Import the required libraries: `json`, `owlready2`
Step 2: Initialize the path to the ontology file and load the ontology.
(i) Append the ontology path.
(ii) Define the ontology file path.
(iii) Load the ontology using the defined file path.
Step 3: Check if the ontology loading was successful.
(i) If the ontology is `None`, print an error message, and exit the program.
Step 4: Try to load the ontology, and if successful:
(i) Open the JSON file containing NVD CVE data (e.g., `nvdcve-1.1.json`).
(ii) Parse the JSON content into a Python dictionary (`data`).
(iii) Iterate through each CVE entry in the data:
(a) Extract CVE ID and description from each entry.
(b) Set properties such as description for each CVE instance.
(c) Create an instance of the `CVE` class for each CVE entry.
- Set the `cve_id` as the individual's name.
- Assign the description to the `description` property of the instance.
- Set other relevant properties accordingly.

Step 5: Save the updated ontology.
Save the updated ontology to `onto_file_path` in RDF/XML format (adjust the format as needed).
Step 6: Print "Ontology updated successfully."
Print a success message if the process is completed without errors, or print an error message if an exception occurs.

(b) ***Method 2:*** **Integrating CVE data with Knowledge Graph (via API)**

There hasn't been any specific integration or support for the NVD (National Vulnerability Database) API in Protégé. Protégé primarily focuses on ontology modeling and management rather than directly interfacing with external data sources like the NVD API. However, with the help of a knowledge graph database like Ontotext GraphDB, semantic data can be stored, and CVE data can be imported through an API into the knowledge graph alongside the existing ontology.

The MIoT semantic model enhances API security by providing security measures, ensuring data is accessed and processed in a meaningful and secure way. Firstly, it validates not just the format, but the semantics of data, ensuring API inputs and outputs are logically consistent with expected meanings. This helps prevent vulnerabilities, where malicious data might bypass traditional validation. Secondly, the semantic model can integrate automated reasoning techniques to detect anomalies or threats based on data patterns and usage behaviour, allowing for early identification of potential security breaches or vulnerabilities.

In this setup, CVE data can be modeled as additional nodes and edges in the knowledge graph, connecting them to relevant nodes representing medical devices or related concepts. This approach leverages the graph database's capabilities for visualization and querying over the integrated data. Additionally, new vulnerabilities introduced into the system can be updated, which is not possible directly in Protégé. This process is further discussed in *Section 7.1.2*, Visualization and Query Interface.

Why are two methods to integrate with NVD

By using both methods, the strengths of each approach can be utilized. For example, to integrate NVD data via Python code focuses on directly integrating CVE data into an ontology format using OWL (Web Ontology Language). This is useful for maintaining a structured and semantically rich representation of the data. This approach seems more suitable for scenarios where the data integration happens at specific intervals or is not required to be updated in real-time. While, Method 2, integration via an API allows for real-time updates and dynamic integration of new vulnerabilities, which is not possible directly in ontology frameworks like Protégé. To integrate NVD information in terms of CVE and CVSS with Knowledge graphs are highly scalable and can handle large datasets efficiently, making them suitable for evolving datasets where new data points are continuously added. in this way, Method 1 ensures a structured and semantically rich integration within an ontology framework, while Method 2 provides the flexibility, scalability, and real-time update capabilities of knowledge graphs.

7.1.1.3 Reasoning Mechanism

With the help of formal methods, the MIoT ontology is evaluated to validate the case study in previous work [13]. However, the MIoT ontology has the potential to revolutionize security automation within healthcare applications by offering a structured framework for representing and understanding the relationships among medical devices, vulnerabilities, and network infrastructure.

By utilizing the predefined concepts and relationships within the MIoT ontology, this study aims to introduce automation capabilities by establishing a ruleset to enable automated reasoning, facilitating more effective inferences and high-level decisions. Additionally, this study implement, visualize, and query this conceptual model in a knowledge graph to store cyber threat intelligence (CTI) for semantic representation and data integration.

With the help of automated reasoning, data are analyzed and stored in a knowledge base to detect potential vulnerabilities and attacks related to medical devices. To perform complex rule-based reasoning in the proposed framework, the following steps are followed, which are specific to the

problem domain and the complexity of the rules involved. Furthermore, the ruleset is applied to the existing knowledge base to perform automated reasoning on it. The evaluation of the ruleset generation is performed by standard knowledge engineering methodology and large language models such as Generative AI models. Table 7.2 illustrates the different steps to perform the reasoning over MIoT ontology.

Table 7.2: Steps to Perform Automated Reasoning

Reasoning Mechanism Steps	
Step	**Description**
1	Define the problem domain
2	Ruleset generation
3	Implement a rule engine or inference system
4	Apply rules on the existing knowledge base
5	Assessment of results

1. Define the Problem Domain

Remote patient monitoring systems are targeted for cyberattacks due to their exposed nature. In such scenarios, maintaining the integrity, confidentiality, and availability of sensitive healthcare data becomes very difficult. Rules-based automated reasoning plays a crucial role in identifying and responding to various situations, including medical emergencies, anomalies in patient data, or security threats. These rules, often expressed in the form of logical or conditional statements, define the conditions under which certain actions should be taken. For example, a rule might specify that if a patient's vital signs exceed certain thresholds (i.e., Rule 1 and Rule 3 in section 1.2.2), an alert should be triggered to notify healthcare providers in terms of inferred axioms. Automated reasoning systems utilize these rules to analyse incoming data from remote patient monitoring devices in real time. By applying logical inference, these systems can quickly assess the data against the established rules and determine whether any action needs to be taken. This process enables timely responses to critical events, such as sending alerts to healthcare professionals or initiating emergency protocols.

By employing sophisticated reasoning mechanisms (i.e., forward chain reasoning), healthcare providers can identify and predict potential vulnerabilities that are exploited by attacks, and their adverse side effects and propose mitigations, consequently affecting the system's performance. Ultimately, the incorporation of automated reasoning mechanisms not only elevates the security standards of remote patient monitoring but also promotes a safer and more secure environment for both patients and healthcare providers, laying the foundation for the continued advancement of remote healthcare technologies.

2. Ruleset Generation

Rule set generation consists of the identification and formularization of rules. Identify the rules or logical constraints that govern the problem domain come from various sources, such as domain

experts, existing knowledge bases, or data-driven analysis. This research adopted the if-then logical approach (A→B) that is usually applied to existing knowledge bases. The first part "A" is called the "antecedent" and the second part "B" is called the "consequent" [245]. Formalizing the rules in a structured format can be easily processed by a computer program. This typically involves representing rules using a formal logic notation, such as first-order (FOL), propositional logic, or rule-based systems like production rules. FOL is a foundational system of logic that allows quantification over objects, enabling more complex expressions than propositional logic. It's a fundamental part of many systems that require detailed logical representation and reasoning. While Propositional Logic is a branch of logic that deals with propositions that can be true or false. It's the basis of logical reasoning in many fields, including computer science and mathematics. In the following section, different rules are proposed that reflect the problem domain in terms of anomalies, vulnerabilities, and attacks on medical devices, their impacts, and their suggested mitigations. The tables show the rule set with its different representations, such as the if-then logical approach, first-order logic, and propositional logic.

Rule 1. ***Detection of high blood pressure reading***

If there is a vulnerability and the blood pressure reading value is updated to more than 120, it is assumed to indicate high blood pressure, and the patient needs attention. In the proposed MIoT ontology, a medical device such as a blood pressure monitor is modelled with the data property hasBloodPressure and assigned a constraint of 120/80 (which is normally 120/80 in adults), as shown in Figure 7.14. If the system is updated with a "140" blood pressure reading, it is assumed to indicate a high blood pressure reading. Whereas Table 7.3 demonstrates its representation in various formats such as If-then logic, First-order logic, and propositional logic.

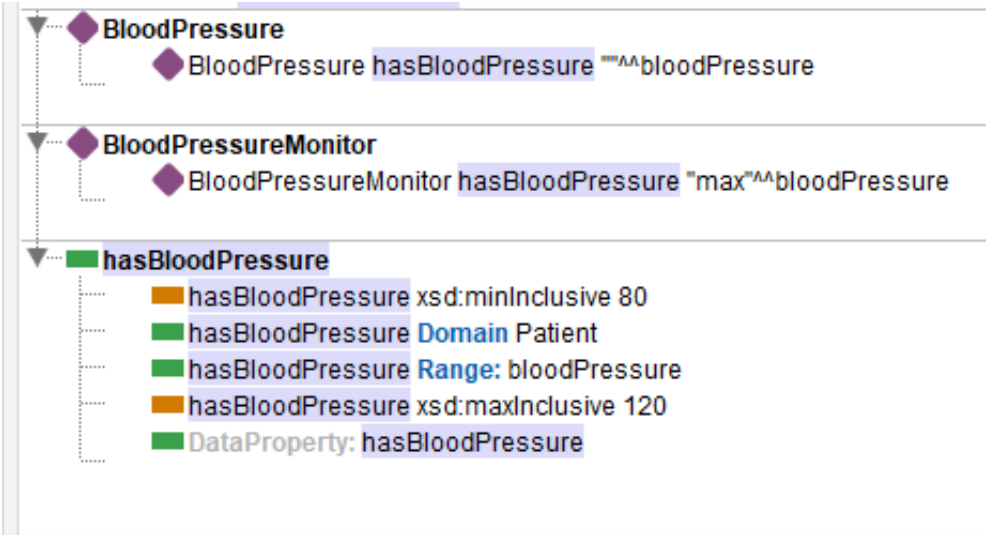

Figure 7.14: The `maxInclusive` and `minInclusive` values for *hasBloodPressure* data property.

Rule 2. ***Data Modification due to Vulnerability***

If any medical device is connected to a network layer through the object property connectedToNetwork and the patient's data is modified, then that device can be considered compromised.

Table 7.3: Detection of High Blood Pressure Reading

Rule 1	
If-then Logic	If there is a medical device that is vulnerable to a specific vulnerability, and there is a blood pressure reading with a reading value that is greater than 120, then infer that it constitutes a high blood pressure reading with a reading value.
First-order Logic	$\forall r, \forall vuln, \forall d, \forall reading\ (BloodPressureReading(r)\ \wedge\ vulnerableTo(d, vuln)\ \wedge\ MedicalDevice(d)\ \wedge\ hasBloodPressure(r, reading) \wedge (reading\ >\ 120)\ \rightarrow\ highBloodPressureReading(r))$
Propositional Logic	$(BloodPressureReading(r)\ \wedge\ vulnerableTo(d, vuln)\ \wedge\ MedicalDevice(d) \wedge hasBloodPressure(r, reading) \wedge (reading > 120)) \Rightarrow HighBloodPressureReading(r)$

In the proposed MIoT ontology, the network layer is connected to a Service, which in turn is connected to Technology (such as Wi-Fi or Cloud) using the object property usingService. This setup increases the risk of a network layer attack if any vulnerability exists. Algorithm 2 outlines the structure of the rule, whereas Table 7.4 demonstrates its representation in various formats such as If-then logic, First-order logic, and propositional logic.

Table 7.4: Data Modification due to Vulnerability

Rule 2	
If-then Logic	If a medical device is connected to a network layer and the network layer has modified data related to a vulnerability, then the medical device is considered compromised with the same vulnerability.
First-order Logic	$\forall d, \forall n, \forall v\ (MedicalDevice(d) \wedge connectedToNetwork(d, n) \wedge hasModifiedData(d, \text{true})\ \wedge\ hasVulnerability(d, v)\ \rightarrow\ compromisedMedicalDevice(d))$
Propositional Logic	$(MedicalDevice(d) \wedge connectedToNetwork(d, networklayer) \wedge hasModifiedData(d, \text{true})\ \wedge\ hasVulnerability(d, vuln))\ \Rightarrow\ CompromisedMedicalDevice(d)$

Rule 3. ***Adverse Side Effects occur due to an increase in Medication Dosage***

In the proposed MIoT ontology, a medical device, such as a DeliverMedication instance of an Infusion Pump, is modelled with the data property usingMedicalDevice and assigned a maximum inclusive value of "10" and a minimum inclusive value of "6", as shown in Figure 7.15. If the system is updated with a dosage value exceeding "10" for a patient, it may cause adverse side effects for the patient. Furthermore, Algorithm 3 defines the structure of the rule, whereas Table 3 shows its representation in various formats such as If-then logic, First-order logic, and propositional logic.

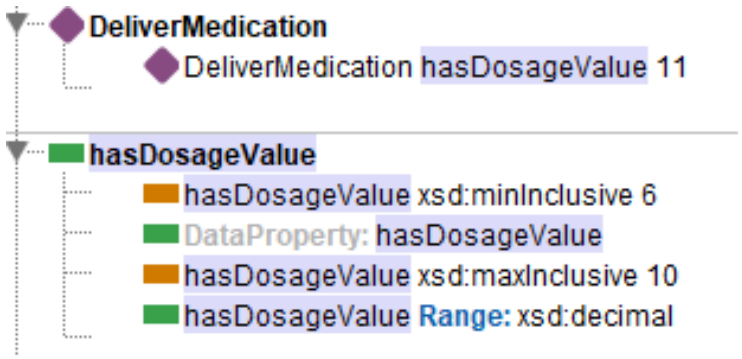

Figure 7.15: The `maxInclusive` and `minInclusive` values for *hasDosageValue* data property.

Table 7.5: Adverse Side Effects occur due to an increase in Medication Dosage

Rule 3	
If-then Logic	If a medication dosage is associated with a patient and the dosage value is greater than 10, then the patient has adverse side effects.
First-order Logic	$\forall p, d, dosage\ (Patient(p) \land usingMedicalDevice(p, d) \land greaterThan(dosage, 10) \rightarrow AdverseSideEffect(p))$
Propositional Logic	$(Patient(p) \land usingMedicalDevice(p, d) \land greaterThan(dosage, 10)) \Rightarrow AdverseSideEffect(p)$

Rule 4. ***Vulnerability Exposure to Exploit***

The MIoT ontology contains two concepts Vulnerability and Exploit. They have inverse properties such as exploitedBy(Vulnerability, Exploit) and hasVulnerability(Exploit, Vulnerability). This rule shows if there exists a vulnerability and an exploit, then it implies that the vulnerability is vulnerable to the exploit. This is a simple strategy that usually occurs in these kinds of scenarios where vulnerabilities are exploited by exploits. Table 7.6 shows its representation in various formats such as If-then logic, First-order logic, and propositional logic.

Table 7.6: Vulnerability Exposure to Exploit

Rule 4	
If-then Logic	If there is a vulnerability and there is an exploit, then the vulnerability is exposed to the exploit.
First-order Logic	$\forall vuln\, \forall exploit\, (V(vuln) \land Exploit(exploit) \rightarrow VulnerableTo(vuln, exploit))$
Propositional Logic	$(Vulnerability(vuln) \land Exploit(exploit)) \Rightarrow vulnerableTo(vuln, exploit)$

Rule 5. ***Vulnerability is exploited by an attack***

This rule extends Rule 4, introducing another concept, ”Attack.” In the MIoT ontology, the concept ”Attack” has relationships with ”Vulnerability” through exploitsVulnerability(Attack, Vulnerability) and with ”Exploit” through hasAttack(Exploit, Attack). This rule states that if there exists a vulnerability and an exploit for that vulnerability, and if that vulnerability is

exploited by a certain attack, then the system with the vulnerability is considered vulnerable to that attack. Table 7.7 shows its representation in various formats such as If-then logic, First-order logic, and propositional logic.

Table 7.7: Vulnerability Considered Vulnerable to Attack

Rule 5	
If-then Logic	If there exists a vulnerability and an exploit, and if that vulnerability is exploited by a certain attack, then the vulnerability is considered to be vulnerable to that attack.
First-order Logic	$\forall vuln\, \forall exploit\, \forall attack\, (Vulnerability(vuln) \land Exploit(exploit) \land exploitedBy(vuln, attack) \rightarrow vulnerableTo(vuln, attack))$
Propositional Logic	$(Vulnerability(vuln) \land Exploit(exploit) \land exploitedBy(vuln, attack)) \Rightarrow vulnerableTo(vuln, attack)$

Rule 6. ***Vulnerability with high severity poses a high risk of attack***

This rule shows the risk of attacks in terms of vulnerability severity. Vulnerability Concept has data property hasSeverity with three values "Low", "Medium" and "High". The hasRiskLevel is the data property of the class AttackRisk with three values, LowRisk, MediumRisk and HighRisk. If there exists a vulnerability and it has severity "high" as indicated by the data property 'hasSeverity', then it infers the existence of an AttackRisk associated with that vulnerability, and the risk level of the vulnerability is considered to be HighRisk. Table 7.8 shows its representation in various formats such as If-then logic, First-order logic, and propositional logic.

Table 7.8: High Risk of Attack for Medical Devices with High Severity

Rule 6	
If-then Logic	If there is a medical device that has a high severity level, then it poses a high risk of attack, and the risk level associated with this medical device is considered high.
First-order Logic	$\forall d\, (MedicalDevice(d) \land hasSeverity(d, high) \rightarrow (AttackRisk(d) \land hasRiskLevel(d, HighRisk)))$
Propositional Logic	$(MedicalDevice(d) \land hasSeverity(d, high)) \Rightarrow (AttackRisk(d) \land hasRiskLevel(d, HighRisk))$

Rule 7. ***Mitigation Recommendation for Vulnerabilities*** The MIoT ontology contains a class Mitigation and MitigationRecommendation under the Countermeasure concept. The class Mitigation has object property hasRecommendation. This Rule suggests that when a vulnerability requires a specific mitigation measure, then a recommendation for that mitigation is generated. It implies a practical response to identified vulnerabilities by proposing corresponding mitigation strategies to address them. Table 7.9 shows its representation in various formats such as If-then logic, First-order logic, and propositional logic.

Table 7.9: Mitigation Recommendation for Vulnerability

Rule 7	
If-then Logic	If there is a vulnerability that requires a certain mitigation, then a mitigation recommendation is made for that mitigation.
First-order Logic	$\forall vuln\, \forall mitigation\, (Vulnerability(vuln) \ \wedge \ hasRecommendation(vuln, mitigation) \ \rightarrow \ MitigationRecommendation(mitigation))$
Propositional Logic	$(Vulnerability(vuln) \wedge hasRecommendation(vuln, mitigation)) \Rightarrow MitigationRecommendation(mitigation)$

Rule 8. ***Mitigation Recommendation for Medical Devices with any Risk Level***

The MIoT ontology contains a class MitigationRecommendation under the Countermeasure concept. The class MedicalDevice has the object property hasRiskLevel with three values: "LowRisk," "MediumRisk," and "HighRisk." This Rule suggests that a mitigation recommendation must be provided for any medical device that has been assigned a risk level. This ensures that all medical devices with identified risks receive appropriate guidance on how to mitigate those risks.

It emphasizes a proactive approach to managing and addressing potential vulnerabilities in medical devices by systematically generating mitigation recommendations based on the assessed risk levels. Table 7.10 shows its representation in formats such as If-then, First-order, and propositional logic.

Table 7.10: Mitigation Recommendation for Medical Devices with Any Risk Level

Rule 8	
If-then Logic	If there is a medical device and it has any risk level, then that medical device requires mitigation.
First-order Logic	$\forall d \forall m\, (MedicalDevice(d) \ \wedge \ hasRiskLevel(d, m) \ \rightarrow \ MitigationRecommendation(d))$
Propositional Logic	$(MedicalDevice(d) \ \wedge \ hasRiskLevel(d, m)) \ \Rightarrow \ MitigationRecommendation(d)$

Summary of Rule Set Generation

The rules presented above carry significant implications for enhancing security within the Internet of Medical Things (IoMT) domain. They serve to protect medical devices and patient's data against vulnerabilities, risks, and potential adverse effects. For example, the first rule detects high blood pressure incidents by correlating vulnerable medical devices with blood pressure readings exceeding 120, thus ensuring timely identification of potential health risks. The second rule addresses the vulnerability of medical devices connected to networks, highlighting the risk of compromise when network-connected devices undergo data modifications due to vulnerabilities. The third rule aids in identifying potential adverse side effects in patients due to high medication dosage. Additionally, subsequent rules further develop vulnerability management strategies by establishing links between vulnerabilities and potential exploits and attacks, identifying high-risk vulnerabilities, and recommending mitigation measures to

strengthen IoMT security infrastructure. Collectively, these rules significantly contribute to enhancing the security posture of IoMT systems, ensuring the safeguarding of medical devices and patient data, and providing the pre-emptive identification and management of potential security threats.

3. Implement a Rule Engine or Inference System

Knowledge-based system consists of two core elements: a knowledge base and an inference engine. The knowledge base contains facts or information about the world, while the inference engine enables the derivation of new knowledge from the existing data. The ability to extract new information is a critical characteristic of every reasoning system and defines its reasoning completeness and soundness. The reasoning process requires dependence on a reference schema containing a catalogue of medical IoT security rules, with each rule representing a vulnerability, exploit, attack or compromised medical device that the system must detect. It is possible by applying the defined rules to the available data using the rule engine or inference system. This may involve chaining together multiple rules, performing logical deductions, or making inferences based on the input data. The most common demonstration involves IF-THEN rules, often coupled with either forward or backward chaining approaches [130]. Once a reasoning engine is chosen, it must be implemented into software (i.e., Protégé). This process entails developing algorithms and data structures capable of efficiently processing the knowledge base and executing the necessary reasoning tasks.

There are many reasoning engines available for ontology models such as Jena[6], Fact++[7], Racer[8], Hermit[9], Pellet[10] and so on. In this work, Pellet., a rule engine or inference system is used, that is capable of applying the defined rules to the problem domain. It is also used to evaluate the consistency checking of the ontology, (Consistency further discussed in Section 1.3.2 (Evaluation)). The Pellet reasoner inference engine uses using forward chain mechanism to control the rules' structure and perform the reasoning on it. Pellet is an OWL-DL reasoner that offers extensive middleware and several unique features while achieving acceptable to very good performance. Additionally, it implements several OWL-DL extensions, such as a combination formalism for OWL-DL ontologies, and preliminary support for OWL/Rule hybrid reasoning [219]. In Protégé current version [246], the Pellet reasoner plugin is already available under the Reasoner Tab and supported for OWL, RDF and XML formats.

[6]https://jena.apache.org/documentation/inference/
[7]http://owl.cs.manchester.ac.uk/tools/fact/
[8]https://www.ifis.uni-luebeck.de/ moeller/racer/
[9]http://www.hermit-reasoner.com/
[10]https://www.w3.org/2001/sw/wiki/Pellet

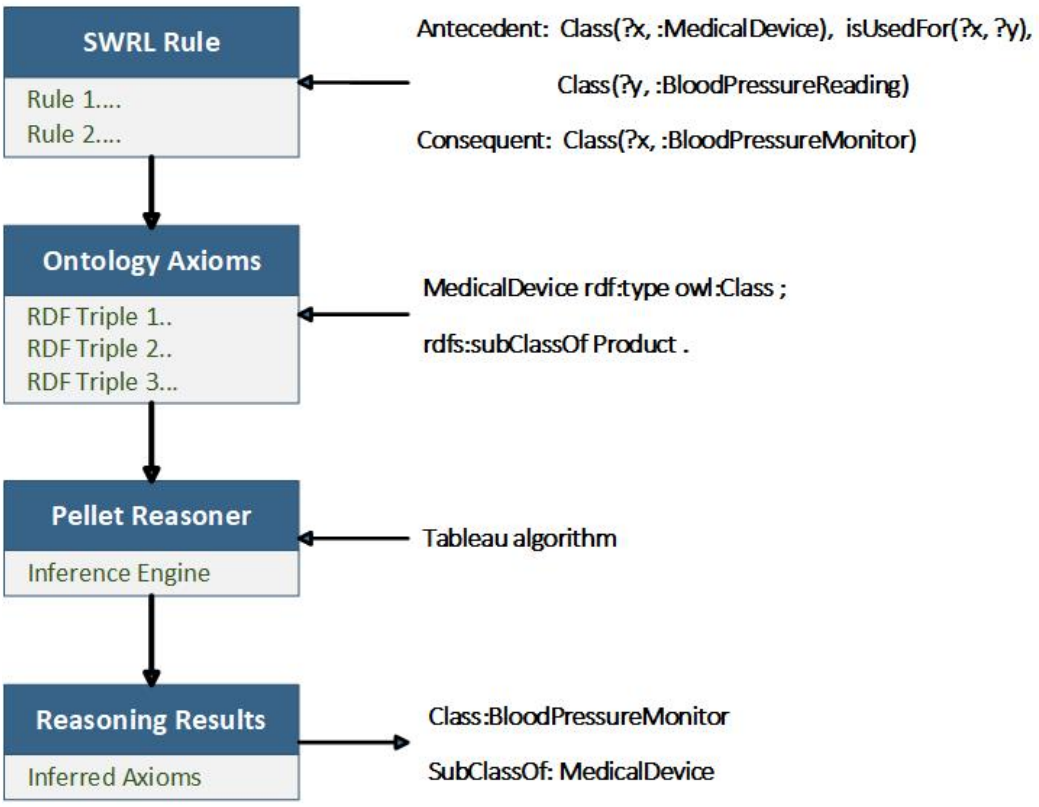

Figure 7.16: Reasoning mechanism by Inference Engine.

This study proposes a set of guidelines for extracting insights from the MIoT ontology, with a focus on areas contributing to logical inference, including modified data, vulnerabilities, exploits, and attacks on medical devices. Evaluating the correctness of a rule engine or inference system involves several critical factors. These include test case validation to ensure the system handles diverse scenarios, logical consistency checks to prevent contradictions, and completeness analysis to verify that all correct inferences are drawn. while performance testing assesses the system's efficiency and scalability. In this work, various techniques were employed to evaluate the rule engine's performance and consistency by testing multiple use cases within the Internet of Medical Things (IoMT) domain.

This work uses the SWRL (Semantic web Rule Language) to implement the rules that are defined in if-then logic in the previous section (Ruleset generation). The protégé application is used to implement the rule set and use the SWRL plugin. These SWRL rules utilize simple syntax comprehensible to both the system and humans [247]. By defining fundamental SWRL rules within the MIoT ontology, and performing reasoning on it, new knowledge is inferred called inferred axioms. SWRL is designed as an extension of OWL, so the standard procedure for executing SWRL rules is to utilize a reasoner compatible with the W3C SWRL specification. Figure 7.16 shows the mechanism for the reasoning process. Each step is defined in detail below:

(a) **SWRL Rule**

SWRL rules are logical rules expressed in the Semantic Web Rule Language. These rules are defined within the ontology to specify additional constraints, relationships, or actions. SWRL rules consist of an antecedent (conditions) and a consequent (actions). These rules, often

expressed in the form of logical statements or conditional statements, define the conditions under which certain actions should be taken. For example, a rule might specify that if a patient's vital signs exceed certain thresholds, an alert should be triggered to notify healthcare providers. SWRL is often chosen over other rule languages like Declarative Logic Programs (DLP) and First Order Classical Logic (FOL) for several reasons such as expressiveness, Support for complex Rule-based reasoning, and alignment with semantic web standards.

Example SWRL rule:

Antecedent:

```
Class(?x, :MedicalDevice),
isUsedFor(?x, ?y),
Class(?y, :BloodPressureReading)
```

Consequent:

```
Class(?x, :BloodPressureMonitor)
```

Annotations:

```
A MedicalDevice used for a BloodPressureReading is a
BloodPressureMonitor.
```

(b) **Ontology Axioms**

Axioms are statements in the ontology that define concepts, properties, and individuals and assert relationships between them. Axioms include class declarations, property declarations, individual declarations, and assertions.

Example ontology axiom:

```
MedicalDevice rdf:type owl:Class ;
              rdfs:subClassOf Product .
```

(c) **Pellet Reasoner**

Pellet is a reasoner for Description logic (DL) and OWL ontologies. It is responsible for processing the ontology and SWRL rules to perform reasoning tasks. Pellet implements algorithms for classification, consistency checking, and instance checking, among others. The Pellet is capable of reasoning with both the ontology axioms and SWRL rules. To validate the reasoning on Pellet reasoner, the rules are created in SWRL (Semantic Web Rule Language). These SWRL rules can be used to demonstrate and infer new data from existing knowledge.

i. ***Inference Engine***

The inference engine within the Pellet Reasoner applies the SWRL rules to derive new knowledge based on the existing ontology axioms. It uses the Tableau algorithm to perform reasoning on the provided ontology axioms and SWRL rules. It evaluates the antecedents of SWRL rules against the ontology to determine when rules are triggered. When a rule is triggered, the inference engine executes the consequent, adding new knowledge to the ontology. By applying logical inference, these systems can quickly assess the data against the established rules and determine whether any action needs to be taken. This process enables timely responses to critical events, such as sending alerts to healthcare professionals or initiating emergency protocols. Finally, the reasoning engine can be seamlessly integrated with other systems and applications to furnish automated reasoning capabilities. For instance, it could be amalgamated with a security monitoring system to furnish automated detection and response to security threats.

(d) **Reasoning Results**

The reasoning results include inferred axioms, new facts, and derived knowledge obtained by applying SWRL rules to the ontology. These results expand the knowledge base of the ontology, allowing it to make new inferences and draw conclusions not explicitly stated in the ontology axioms.

```
Class: BloodPressureMonitor
SubClassOf: MedicalDevice
```

These steps are generally taken by an inference engine to perform reasoning over an existing knowledge base, enabling it to infer hidden facts from the knowledge base. This process involves applying logical rules and ontology axioms to uncover implicit relationships and properties, ultimately enriching the knowledge base with new, deduced information that was not explicitly stated before.

4. Apply Rules on the existing Knowledge Base

The rules are proposed in an If-then logic representation (Section 2. Ruleset Generation). In this phase, these rules are converted into SWRL format to be implemented and executed in Protégé, where the MIoT ontology is imported along with NVD individuals. Table 7.11 provides an outline of these rules, including their SWRL syntax and descriptions. This process ensures that the rules can be effectively applied within the semantic model, enabling automated reasoning and the inference of new knowledge from the existing data.

Table 7.11: SWRL Rules and their Descriptions

SWRL Rules with Descriptions		
Rule	**SWRL Rule**	**Description**
Rule 1	`BloodPressureReading(?r), vulnerableTo(?d, ?vuln), MedicalDevice(?d), hasReadingValue(?r, ?reading), greaterThan(?reading, 120) -> HighBloodPressureReading(?r)`	This rule states that if a medical device (denoted as 'd') is vulnerable to a certain vulnerability ('vuln'), and a blood pressure reading (denoted as 'r') is recorded such that the reading exceeds 120, it is inferred to be a high blood pressure reading.
Rule 2	`MedicalDevice(?d), connectedToNetwork(?d, ?networklayer), hasModifiedData(?d, true), hasVulnerability(?d, ?vuln) -> CompromisedMedicalDevice(?d)`	This rule states that if a medical device is connected to a network layer, the data on that network layer is modified (indicating a potential security breach), and the medical device has a vulnerability, then the medical device is inferred to be compromised.
Rule 3	`Patient(?p), usingMedicalDevice(?p, ?d), greaterThan(?dosage, 10) -> AdverseSideEffect(?p)`	This rule states that if a patient is using a medical device and the dosage of medication is greater than 10, then it is inferred that the patient may experience an adverse side effect.
Rule 4	`Vulnerability(?vuln), Exploit(?exploit) -> vulnerableTo(?vuln, ?exploit)`	This rule states that if a vulnerability exists and there is an exploit that targets it, then the vulnerability is considered to be vulnerable to that exploit.
Rule 5	`Vulnerability(?vuln), Exploit(?exploit), exploitedBy(?vuln, ?attack) -> vulnerableTo(?vuln, ?attack)`	This rule states that if there exists both a vulnerability and an exploit, and the vulnerability is exploited by an attack, then the vulnerability is vulnerable to that attack.

Table 7.11: SWRL Rules and their Descriptions (continued)

Rules with Descriptions		
Rule	**SWRL Rule**	**Description**
Rule 6	`MedicalDevice(?d), hasSeverity(?d, "high") -> AttackRisk(?d), hasRiskLevel(?d, HighRisk)`	This rule assesses the risk level based on the severity of vulnerabilities. If the vulnerability severity is high, the risk of attack will be high.
Rule 7	`MedicalDevice(?d), hasSeverity(?d, "high") -> AttackRisk(?d), hasRiskLevel(?d, HighRisk)`	This rule suggests mitigation measures for specific vulnerabilities. If a vulnerability has a recommended mitigation action, then that action is considered a MitigationRecommendation.
Rule 8	`MedicalDevice(?d), hasRiskLevel(?d, ?m) -> MitigationRecommendation(?d)`	This rule suggests that if a medical device has any risk level, then the medical device needs a mitigation recommendation.

Figure 7.17 shows the implemented SWRL rules in Protégé. It lists a set of rules written in SWRL (Semantic Web Rule Language) format. Each rule consists of an antecedent (the ”if” part) and a consequent (the ”then” part), defining logical conditions and their corresponding actions or conclusions.

The reasoning process is conducted using an inference engine (i.e., Pellet reasoner). The results are presented in the following section (i.e., ’Inferred Axioms after Reasoning’), which displays the output of each SWRL rule in terms of the inferred axioms added to the existing knowledge base. Additionally, a description of each rule is provided to explain its purpose and impact. The figures below illustrate the rules, the data in the knowledge base, and the inferred axioms resulting from the reasoning process.

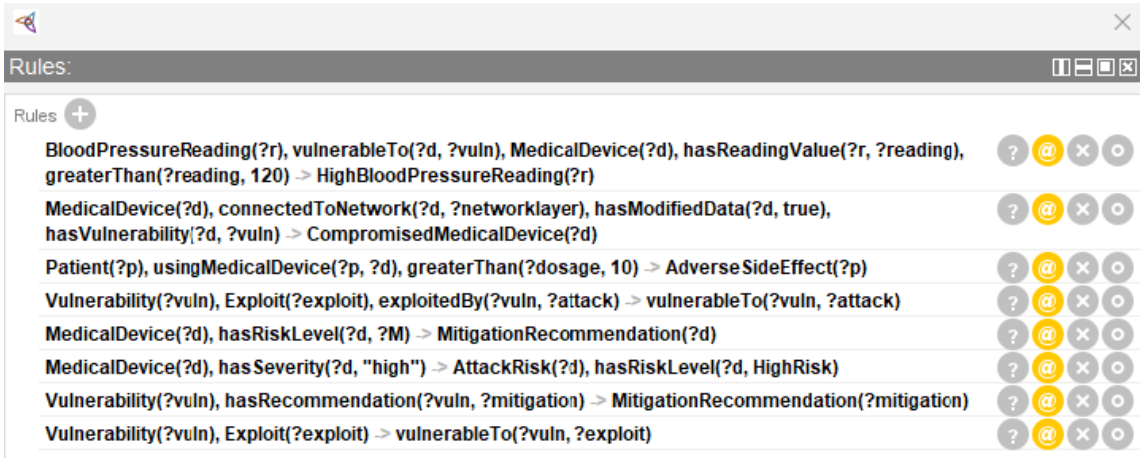
Rules:
Rules
BloodPressureReading(?r), vulnerableTo(?d, ?vuln), MedicalDevice(?d), hasReadingValue(?r, ?reading), greaterThan(?reading, 120) -> HighBloodPressureReading(?r)
MedicalDevice(?d), connectedToNetwork(?d, ?networklayer), hasModifiedData(?d, true), hasVulnerability(?d, ?vuln) -> CompromisedMedicalDevice(?d)
Patient(?p), usingMedicalDevice(?p, ?d), greaterThan(?dosage, 10) -> AdverseSideEffect(?p)
Vulnerability(?vuln), Exploit(?exploit), exploitedBy(?vuln, ?attack) -> vulnerableTo(?vuln, ?attack)
MedicalDevice(?d), hasRiskLevel(?d, ?M) -> MitigationRecommendation(?d)
MedicalDevice(?d), hasSeverity(?d, "high") -> AttackRisk(?d), hasRiskLevel(?d, HighRisk)
Vulnerability(?vuln), hasRecommendation(?vuln, ?mitigation) -> MitigationRecommendation(?mitigation)
Vulnerability(?vuln), Exploit(?exploit) -> vulnerableTo(?vuln, ?exploit)

Figure 7.17: Ruleset implementation in Protégé desktop application .

(a) **Rule 1:** Detection of high blood pressure reading

Rule 1 states that if a blood pressure reading (?r) is associated with a vulnerability (?vuln) in a medical device (?d), and the reading value is greater than 120, then it is inferred to be a high blood pressure reading. Figure 7.18 shows details related to the individual `"BloodPressureReading1"` within the MIoT ontology, which has a reading value of 140. According to the rule, it infers that the individual `"BloodPressureReading1"` is considered to be a ”HighBloodPressureReading,” as shown in the left panel of the figure.

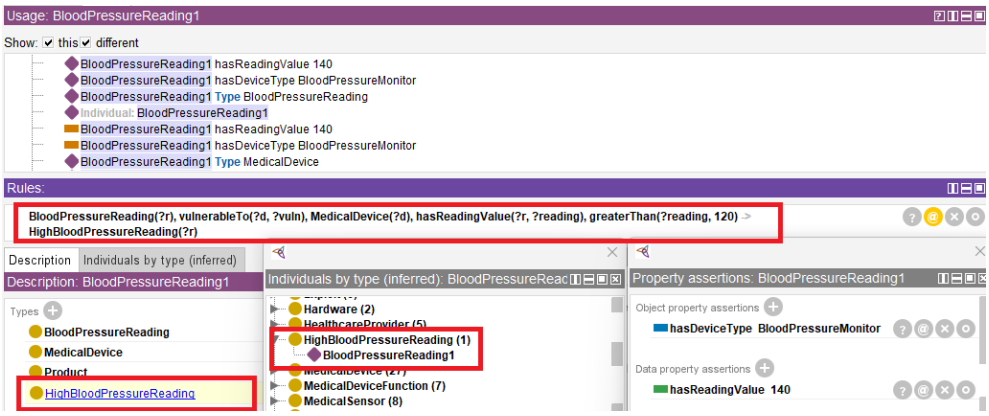

Figure 7.18: Rule 1: The inferred axiom shown as `"HighBloodPressureReading"`.

(b) **Rule 2:** Data Modification due to Vulnerability

Rule 2 states that if a medical device (?d) is connected to a network (?networklayer), has modified data (?d, true), and has a vulnerability (?vuln), then it is inferred to be a compromised medical device. Figure 7.19 shows details related to the individual ”Pacemaker” within the MIoT ontology. This individual is associated with several vulnerabilities and has modified data. According to the rule, it infers that the individual ”Pacemaker” is considered to be a ”CompromisedMedicalDevice,” as shown in the Types Section of the figure. Similarly, a few more medical devices are also compromised when this rule is triggered such as ”Defibrillator” and ”ImplantableCardiacMonitor”.

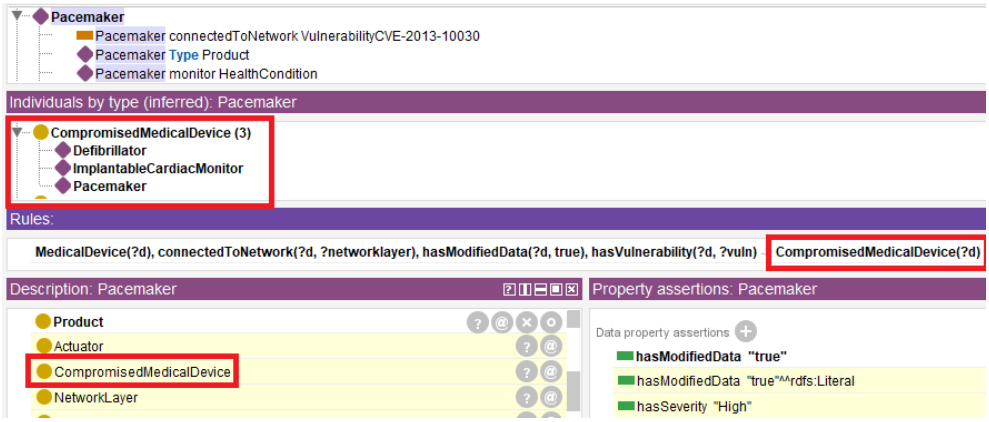

Figure 7.19: The inferred axiom shown as ”CompromisedMedicalDevice”.

(c) **Rule 3:** Adverse Side Effects occur due to an increase in Medication Dosage

Rule 3 states that if a patient (?p) is using a medical device (?d), and the dosage is greater than 10, then it is inferred that the patient will experience an adverse side effect. Figure 7.20 shows details related to the individual ”John” as a `Patient` within the MIoT ontology, who is using an infusion pump and has a dosage value greater than 10. According to the rule, it is inferred that the individual ”John” will experience an `AdverseSideEffect`.

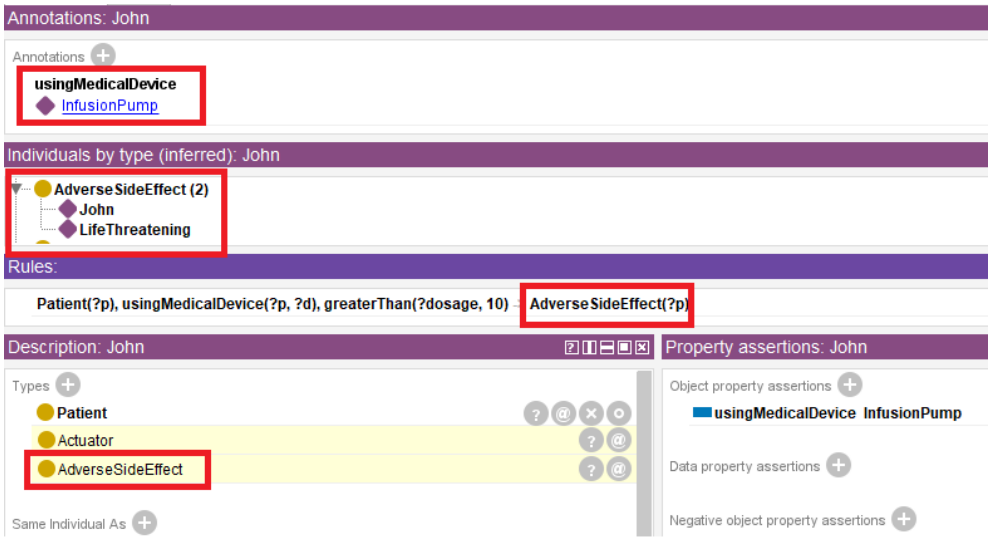

Figure 7.20: The inferred axiom shown as ”AdverseSideEffect”.

Additionally, a function `DeliverMedication`, is `monitoredBy` the individual `InfusionPump`. Figure 7.21 shows the individual ”DeliverMedication” being monitored by an infusion pump. After triggering the rule, it infers that the `MedicationDosage` is affected.

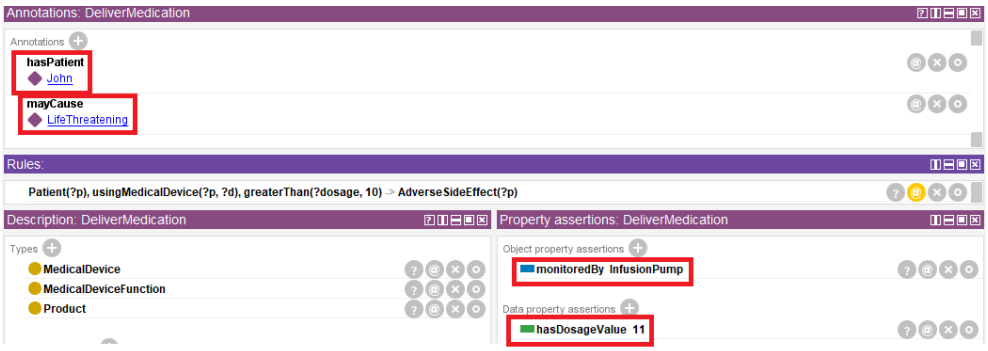

Figure 7.21: The inferred axiom for `DeliverMedication` shows the `LifeThreatening`.

(d) **Rule 4:** Vulnerability Exposure to Exploit

Rule 4 states that if a vulnerability (?vuln) is associated with an exploit (?exploit), then it is inferred that the vulnerability is exposed to the exploit. The Figure 7.22 shows details related to the individual ”VulnerabilityCVE-2010-10010” within the MIoT ontology. This individual is associated with multiple exploits and medical devices, indicating its vulnerability status.

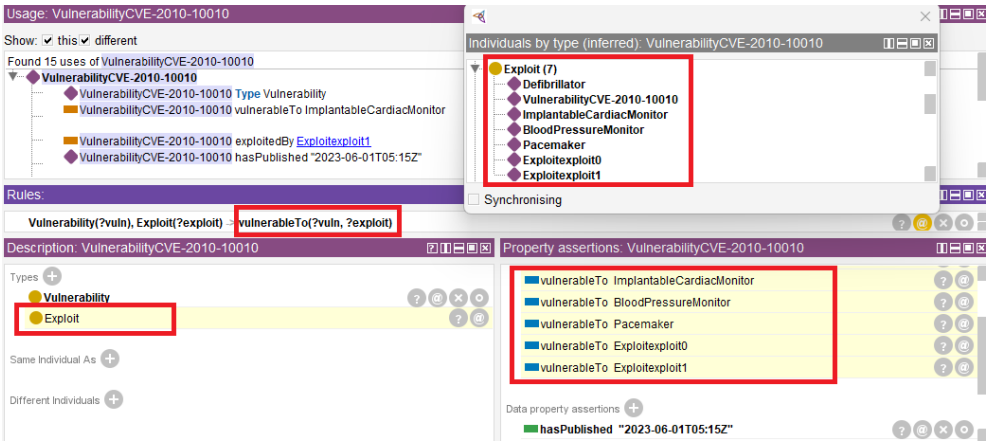

Figure 7.22: The inferred axiom shown as ”Exploit”.

(e) **Rule 5:** Vulnerability is exploited by an attack

Rule 5 states that if a vulnerability (?vuln) is associated with an exploit (?exploit) and is exploited by an attack (?attack), then it is inferred that the vulnerability is exposed to the attack. Figure 7.23 shows details related to the individual ”VulnerabilityCVE-2013-10029” within the MIoT ontology. This individual is associated with multiple exploits and medical devices (i.e., Defibrillator), indicating its vulnerability status. According to the rule, it infers that the individual `"VulnerabilityCVE-2013-10029"` exploits the attack `DenialOfServiceAttack`.

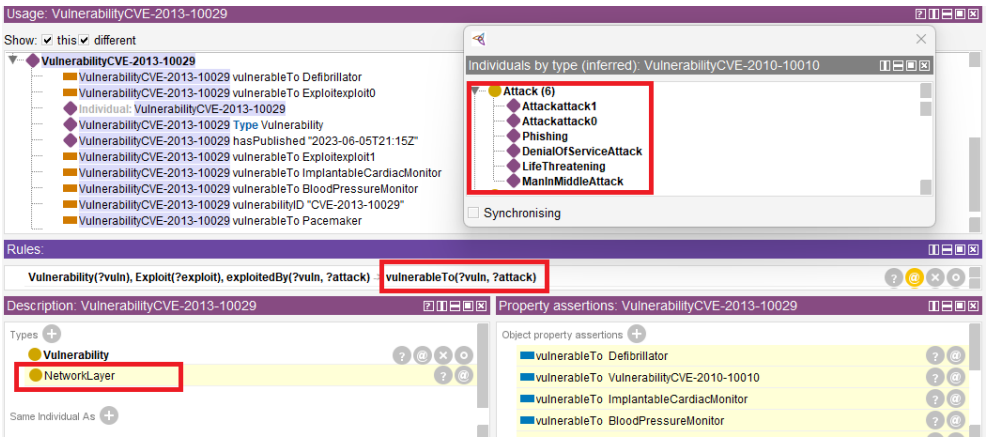

Figure 7.23: The inferred axiom shown as `NetworkLayer` attacks for "VulnerabilityCVE-2013-10029"

(f) **Rule 6:** Vulnerability with high severity poses a high risk of attack

Rule 6 states that if a medical device (?d) has a severity level (?d, "high"), then it is inferred that the device has a high attack risk and a high-risk level. Figure 7.24 shows details related to the individual "Defibrillator" within the MIoT ontology. This individual is associated with various vulnerabilities, exploits, and medical device types. According to the rule, it infers that the individual `Defibrillator` has a high `AttackRisk`.

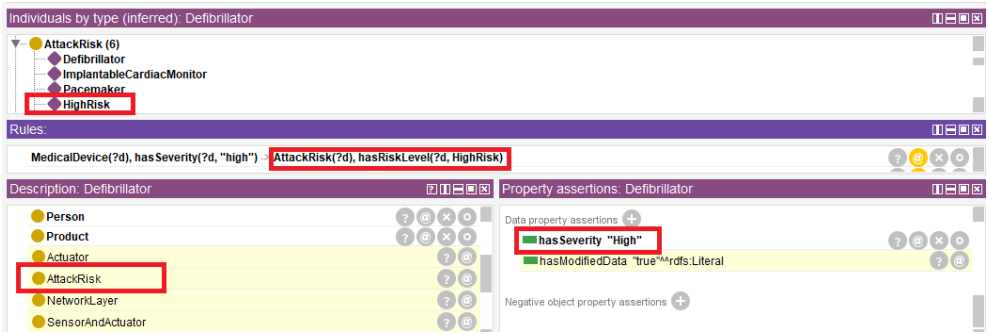

Figure 7.24: The inferred axiom shown as hasRiskLevel `HigHRisk` due to "high Severity".

(g) **Rule 7:** Mitigation Recommendation for Vulnerabilities

Rule 7 states that if a vulnerability (?vuln) has a recommendation (?mitigation), then it is inferred that there is a mitigation recommendation for the vulnerability. Figure 7.25 indicate that the vulnerability "VulnerabilityCVE-2021-31233" within the MIoT ontology hasRecommendaed Mitigation. This individual is associated with multiple exploits, medical devices, and has a mitigation recommendation to install software updates. According to the rule, it infers that the individual `VulnerabilityCVE-2021-31233` has a `MitigationRecommendation`.

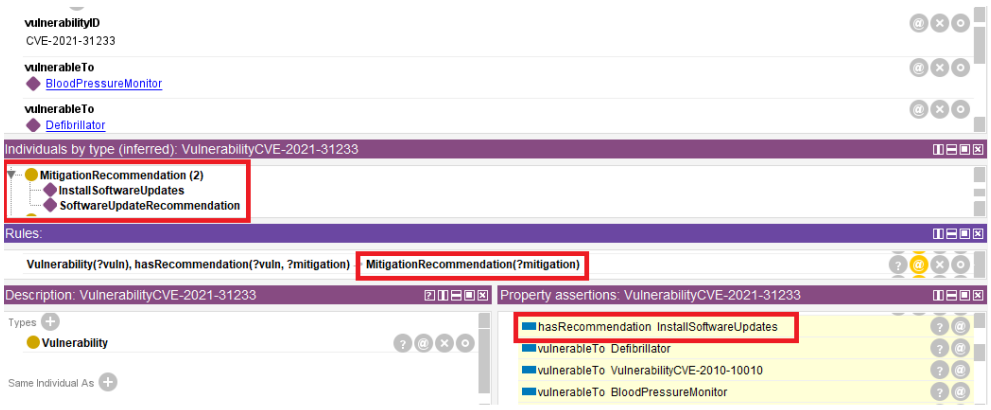

Figure 7.25: The MitigationRecommendations suggested for `VulnerabilityCVE-2021-31233`.

To further look at details, the `InstallSoftwareUpdate` is a type of MitigationRecommendation, shown as in Figure 7.26.

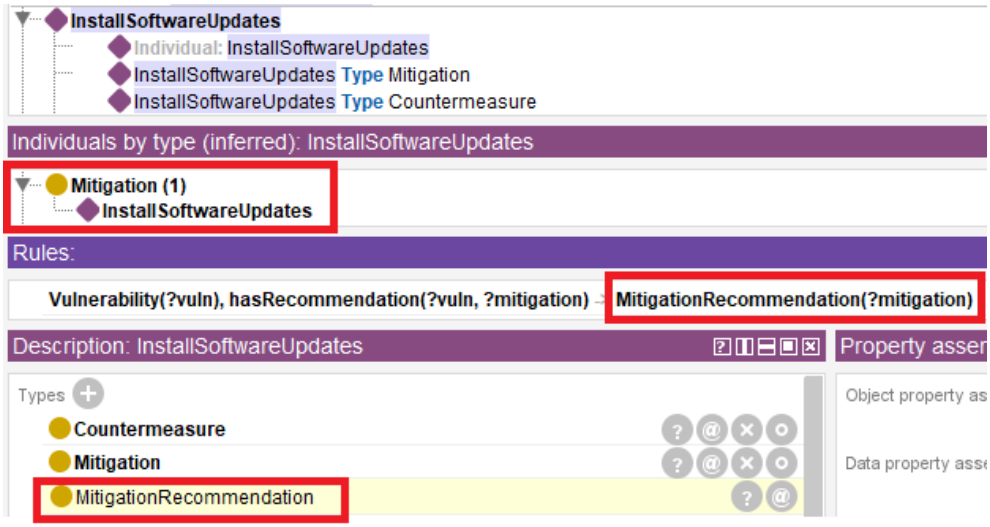

Figure 7.26: The InstallSoftwareUpdate inferred axiom shown as MitigationRecommendation.

(h) **Rule 8:** Mitigation Recommendation for Medical devices with any Risk Level

Rule 8 is very interesting and shows that if a medical device (?d) has a risk level (?m), then it is inferred that there is a mitigation recommendation for that device. Figure 7.27 shows details related to the individual ”Pacemaker” within the MIoT ontology. This individual is connected to the network and has several vulnerabilities, including ”VulnerabilityCVE-2013-10030” and ”VulnerabilityCVE-2010-10010,” as well as a high-risk level. This rule infers the `MitigationRecommendation`, identify `ATtackRisk` as well. According to the rule, it infers that the individual ”Pacemaker” requires a mitigation recommendation.

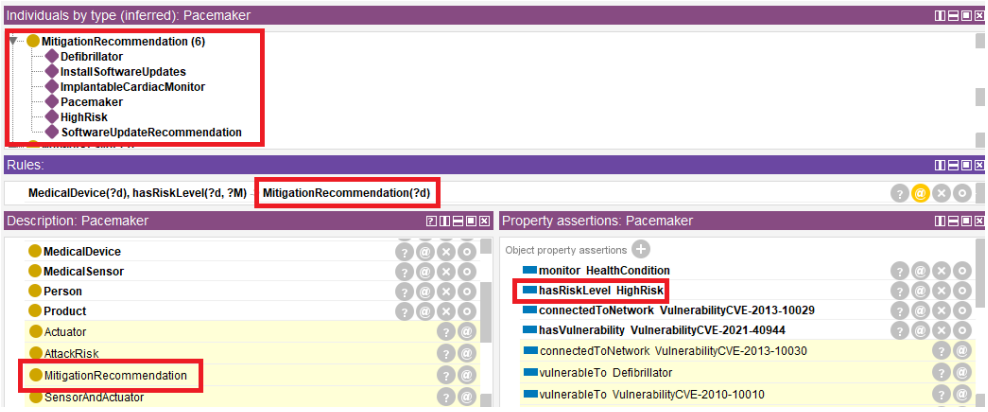

Figure 7.27: The medical device `Pacemaker` has `MitigationRecommendation` is suggested due to `HighRisk`.

However, the reasoning is performed on the entire ruleset, so all the rules are triggered, inferring new facts in the knowledge base. This is why some outputs may appear similar (e.g., Rule 7 and Rule 8). If the rules were run independently, different results would be shown.

5. Assessment of results

The objective of this study is not only to generate the rules individually but to perform reasoning over data to automatically identify different aspects related to security. The study aims to provide a comprehensive security mechanism through automated reasoning, observing how the rules work together to provide information about anomalies, vulnerabilities, exploits, and attacks in the remote patient monitoring setting. Additionally, the study seeks to offer mitigation recommendations to secure the system and ensure the Confidentiality, Integrity, and Availability (CIA) of the data.

7.1.2 Visualization and Query Interface

The results indicate that the issue of overlapping nodes and edge crossings persists when representing large ontologies through node-link diagrams such as OntoGraph[11] and OWLViz[12], which are Protégé plug-ins. These tools encounter challenges when dealing with large ontologies and offer limited interaction capabilities regarding predicates. Furthermore, there is a scarcity of solutions for visualizing the instance level. Features like zooming, filtering, and details-on-demand are not widely available in most tools. Consequently, it is often not feasible to emphasize certain concepts while de-emphasizing others within the ontology. Additionally, the exploration of multiple and synchronized views for presenting schema and/or instances of ontologies is rarely undertaken.

Therefore, this study uses a knowledge graph database, such as Ontotext GraphDB[13], to store and visualize data from the MIoT ontology. For this purpose, RDF triples are imported into the knowledge graph alongside NVD API data. CVE data is modeled as additional nodes and edges in the knowledge graph, connected to the relevant nodes representing medical devices, vulnerabilities, or related concepts.

[11] https://protegewiki.stanford.edu/wiki/OntoGraf
[12] https://protegewiki.stanford.edu/wiki/OWLViz
[13] https://www.ontotext.com/products/graphdb/

This approach leverages the graph database's capabilities for visualizing and querying the aggregated data.

7.1.2.1 Knowledge Graph Visualization

For visualization, this study uses Ontotext GraphDB[14], a graph database compliant with W3C standards such as RDF [248] and SPARQL [153]. Furthermore, as outlined in the previous section (1.2.2.2 Integration with NVD Database), the incorporation of CVE data into the knowledge graph entails retrieving information via the NVD API[15]. This CVE data is then integrated with a semantic model into the Medical Internet of Things Knowledge Graph (MIoT KG) to store cyberthreat Intelligence (CTI). This integration relies on establishing mappings between the concepts defined in the MIoT ontology and the entries within the NVD database. Table 7.12 provides a detailed overview of these mappings, illustrating the relationship between MIoT ontology elements and their counterparts in the NVD database.

Table 7.12: Mappings between MIoT Ontology and NVD Database

MIoT Ontology Properties and NVD Database Entry Mapping	
MIoT Ontology Properties	**NVD Database Entry**
Vendor.hasTakenBy	references > reference_data > tags > Vendor Advisory
Product.hasName	references > reference_data > tags > Product
Weakness.hasCweId	problemtype > problemtype_data > description > value
Vulnerability.hasVulnerabilityID	cve > CVE_data_meta > ID
Vulnerability.hasPublished	publishedDate
Attack.hasAffect	impact > baseMetricV3 > cvssV3 > attackComplexity
Exploit.hasExploitabilityScore	impact > exploitabilityScore
Vulnerability.hasSeverity	impact > baseMetricV3 > cvssV3 > baseSeverity
Vulnerability.hasAvailabilityImpact	impact > baseMetricV3 > cvssV3 > availabilityImpact
Vulnerability.hasIntegrityImpact	impact > baseMetricV3 > cvssV3 > IntegrityImpact
Vulnerability.hasConfidentialityImpact	impact > baseMetricV3 > cvssV3 > ConfidentialityImpact

After mapping the relevant properties from MIoT ontology and NVD CVE data, the knowledge graph is ready for storage and visualization of data. Here are few concepts are visualized as an example in GraphDB. Figure 7.28 shows the Concept Product in Ontotext graphDB. This Figure illustrates the main class node and their relationships in the form of implicit and explicit nodes. Similarly, Figure 7.29 shows the Vulnerability class node and their predicates.

[14]https://graphdb.ontotext.com/
[15]Application Programming Interface

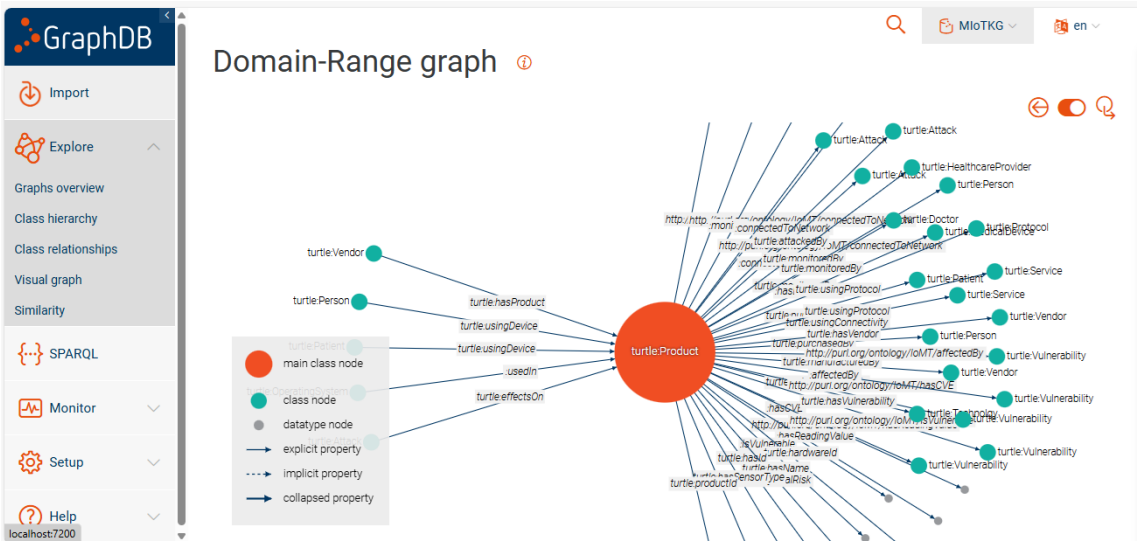

Figure 7.28: Domain-Range graph for the concept `Product` .

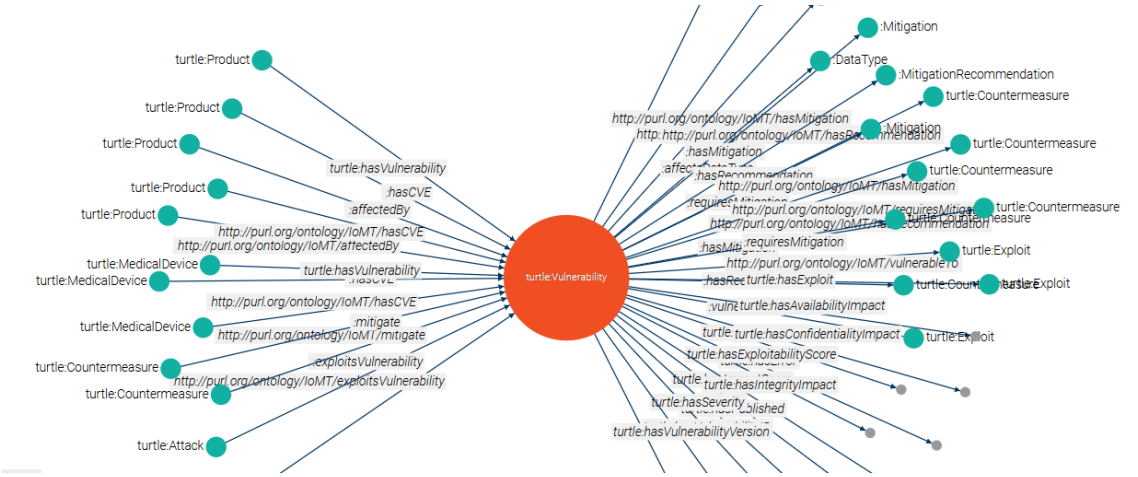

Figure 7.29: Domain-Range graph for the concept `Vulnerability` .

This domain-range graph shows the interconnection between different nodes and provides information about their related classes, predicates, and how these are connected. This detailed information is not visible through OWL viz or OntoGraph in Protégé.

To further elaborate and get information about CIA for any particular vulnerability, the node information is visualized as shown in Figure 7.30. It shows the Pacemaker is an individual for the Concept MedicaSensor and its related entities and the particular vulnerability impact in terms of ConfidentialityImpact, IntegrityImpact, AvaliabilityImpact. To explore it further and get information about the related entities for the individual Pacemaker, kG can facilitate to expand it to the level of n-nodes as shown in Figure 7.31.

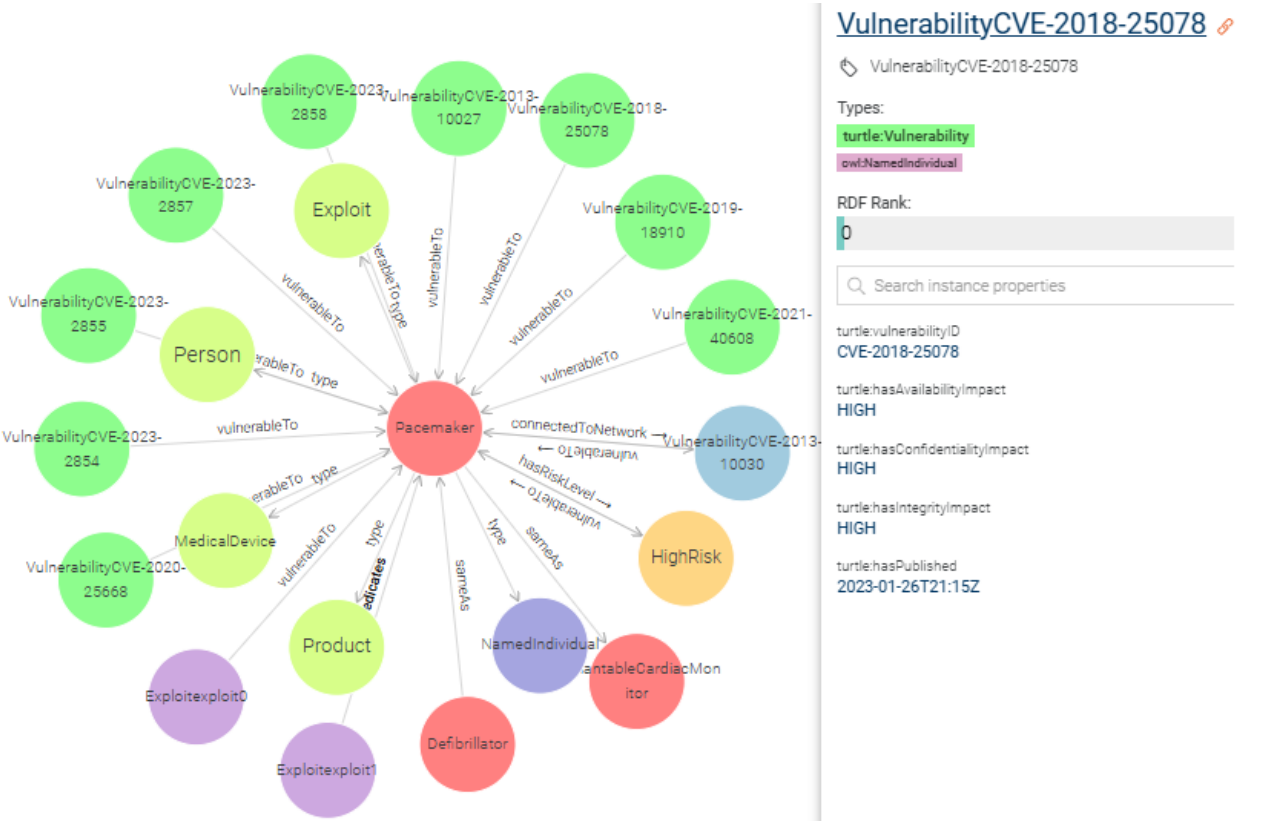

Figure 7.30: The individual `Pacemaker` with CIA information .

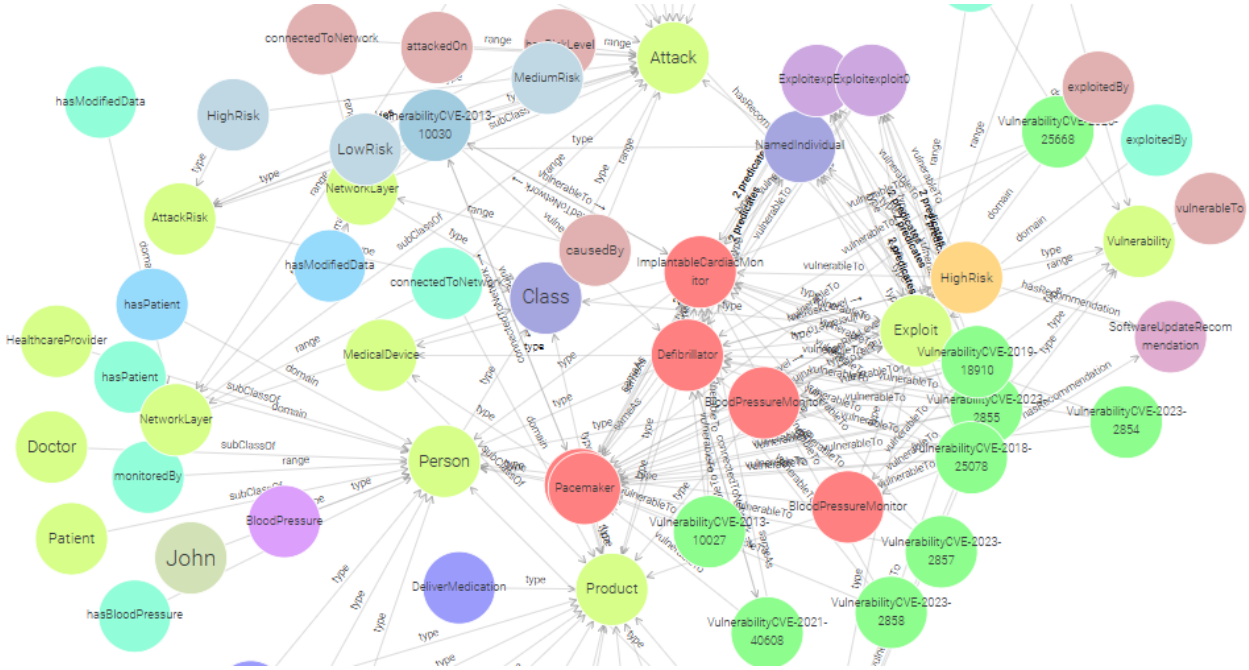

Figure 7.31: The individual `Pacemaker` extended with the information about related entities .

7.1.2.2 SPARQL Endpoint

To evaluate the efficiency of the developed semantic framework using the SPARQL query language. SPARQL, a semantic query language, is used to retrieve and manipulate data stored in the Resource Description Framework (RDF) format. The Ontograph DB supports a SPARQL endpoint for data

retrieval, updating, and deletion. To access data in the Medical Internet of Things (MIoT) Knowledge Graph (KG), this study formulated several queries to address the competency questions (CQs) proposed in *Chapter 4*. These queries are designed to retrieve data from the knowledge graph (KG), which is then verified to determine whether the semantic framework meets the specified criteria addressed in the form of competency questions (CQs).

i. Competency Questions and Their Expected Results

Following SPARQL query results shows the robust performance by fulfiling the requirements of Competency Questions **(CQs)** specified in the initial phase of ontology development.

CQ(a). **What types of devices are utilized in the IoMT environment?**

Various medical devices are utilized within the Internet of Medical Things (IoMT) environment. The types of medical devices that are modeled within the ontology, as identified using SPARQL queries, are illustrated in Figure 7.32.

SPARQL Query 1

```
SELECT ?Device
WHERE {
   ?Device a turtle:MedicalDevice .
}
```

Device
BloodPressureMonitor
BloodPressureReading1
BloodPressureReading2
Pacemaker
Defibrillator

Figure 7.32: `MedicalDevice` used in IoMT environment.

Similarly, to further make it complex to see the medical devices along with their related products. The following query is presented and results shown in Figure 7.33.

SPARQL Query 2

```
SELECT ?Product ?MedicalDevice
WHERE {
  ?Product :hasDeviceType ?MedicalDevice .
}
```

Product	MedicalDevice
CardiacRhythmManagement	ImplantableCardiacMonitor
CardiacRhythmManagement	RemoteMonitoringSystem
CardiacRhythmManagement	Pacemaker
GlucoseMonitoringSystem	FreeStyleLibreSensor
D40G	BloodPressureMonitor
GTel	GlucoseMonitoringSystem
Foracare	ForaTeleHealthSoftware
ComarchHomeHealth	Glucometer

Figure 7.33: `MedicalDevice` along with their `Product`.

CQ(b). **Who are the vendors of medical devices?**

The MIoT ontology contains various popular vendors in the field of IoMT. The following SPARQL query shows the various vendors and output shown in Figure 7.34. To make it more complex and see the related medical devices with those vendors, the SPARQL query 4 is proposed and the result shown in Figure 7.35

SPARQL Query 3

```
SELECT ?Vendor
WHERE {
    ?Vendor a turtle:Vendor .
}
```

Vendor
Abbott
AliveTech
Comarch
Foracare
MySignals
NeuroTech
Omran
Philips

Figure 7.34: List of `Vendor` used in IoMT.

SPARQL Query 4

```
SELECT Distinct ?MedicalDevice ?Product ?Vendor
WHERE {
  ?Product :hasDeviceType ?MedicalDevice .
  ?Vendor :hasProduct ?Product .
  }
```

MedicalDevice	Product	Vendor
ImplantableCardiacMonitor	CardiacRhythmManagement	Abbott
RemoteMonitoringSystem	CardiacRhythmManagement	Abbott
Pacemaker	CardiacRhythmManagement	Abbott
Glucometer	ComarchHomeHealth	Comarch
BloodPressureMonitor	D40G	Foracare

Figure 7.35: `MedicalDevice`, `Product` and their `Vendor`.

CQ(c). **What firmware, version, operating system, software, or applications are utilized in manufacturing medical devices?**

The following query is designed to retrieve information about various medical devices and their associated properties, such as operating systems, communication protocols, and connectivity types. Figure 7.36 output illustrates the description of the **CQ(c)**.

SPARQL Query 5

```
SELECT ?MedicalDevice ?OperatingSystem ?Protocol ?Technology
WHERE {
  ?MedicalDevice :usingOS ?OperatingSystem .
  ?MedicalDevice :usingProtocol ?Protocol .
  ?device :usingConnectivity ?Technology .
}
```

MedicalDevice	OperatingSystem	Protocol	Technology
WearableTherapeuticToolForAutism	Android	BLE	Bluetooth
WearableTherapeuticToolForAutism	AppleIoS	BLE	Bluetooth
Wearable6LeadEKG	Android	BLE	Bluetooth
Wearable6LeadEKG	AppleIoS	BLE	Bluetooth
WearableTherapeuticToolForAutism	Android	MQTT	Bluetooth
WearableTherapeuticToolForAutism	AppleIoS	MQTT	Bluetooth

Figure 7.36: `MedicalDevice` with their `OperatingSystem`, `Protocol` and `Technology` used.

CQ(d). **What kind of vulnerabilities are potentially presented in specific IoMT devices?**

The following query highlights various vulnerabilities within the semantic framework. Due to the large number of vulnerability instances, the query is limited to some records. The output of the query is shown in Figure 7.37.

SPARQL Query 6

```
SELECT ?Vulnerability
WHERE {
    ?Vulnerability a turtle:Vulnerability .
}
LIMIT 20
```

Vulnerability
VulnerabilityCVE-2013-10029
VulnerabilityCVE-2013-10030
VulnerabilityCVE-2013-1860
VulnerabilityCVE-2014-0177
VulnerabilityCVE-2014-125101
VulnerabilityCVE-2014-125102
VulnerabilityCVE-2015-10111
VulnerabilityCVE-2015-10113
VulnerabilityCVE-2015-10114
VulnerabilityCVE-2015-10115
VulnerabilityCVE-2015-10116
VulnerabilityCVE-2015-10117
VulnerabilityCVE-2015-10125

Figure 7.37: List of vulnerabilities present in IoMT devices .

CQ(e). **Are any of the medical devices vulnerable in a remote patient monitoring setting?**

Initially, by running SPARQL Query 7(1), this study obtained five records, as shown in Figure 7.38. These records represent devices connected to a network that have the hasDeviceType property. To satisfy the requirement for CQ (e), which is to determine whether any device is vulnerable, it made the query more complex to specifically check for vulnerabilities in medical devices. Query 7(2) was updated to include the `isVulnerable` property with the value true. This refined query returned only the four records identified as vulnerable, as shown in Figure 7.39.

SPARQL Query 7(1)

```
SELECT ?Vulnerability ?VulnerabilityID ?MedicalDevice ?Product
WHERE {
    ?Vulnerability a base:Vulnerability .
    ?Vulnerability base:vulnerabilityID ?VulnerabilityID .
    ?Product :hasDeviceType ?MedicalDevice .
    ?MedicalDevice :connectedToNetwork ?Vulnerability .
   }
```

Vulnerability	VulnerabilityID	MedicalDevice	Product
VulnerabilityCVE-2013-10030	'CVE-2013-10030'	ImplantableCardiacMonitor	CardiacRhythmManagement
VulnerabilityCVE-2010-3856	'CVE-2010-3856'	FreeStyleLibreSensor	GlucoseMonitoringSystem
VulnerabilityCVE-2013-10027	'CVE-2013-10027'	Glucometer	ComarchHomeHealth
VulnerabilityCVE-2013-10027	'CVE-2013-10027'	Glucometer	Liblium
VulnerabilityCVE-2013-10030	'CVE-2013-10030'	Pacemaker	CardiacRhythmManagement

Figure 7.38: MedicalDevice that are *not vulnerable* .

SPARQL Query 7(2)

```
SELECT ?Vulnerability ?VulnerabilityID ?MedicalDevice ?Product
WHERE {
    ?Vulnerability a base:Vulnerability .
    ?Vulnerability base:vulnerabilityID ?VulnerabilityID .
    ?Product :hasDeviceType ?MedicalDevice .
    ?MedicalDevice :connectedToNetwork ?Vulnerability .
    ?MedicalDevice :isVulnerable true .
}
```

Vulnerability	VulnerabilityID	MedicalDevice	Product
VulnerabilityCVE-2010-3856	'CVE-2010-3856'	FreeStyleLibreSensor	GlucoseMonitoringSystem
VulnerabilityCVE-2013-10027	'CVE-2013-10027'	Glucometer	ComarchHomeHealth
VulnerabilityCVE-2013-10027	'CVE-2013-10027'	Glucometer	Liblium
VulnerabilityCVE-2013-10030	'CVE-2013-10030'	Pacemaker	CardiacRhythmManagement

Figure 7.39: `MedicalDevice` that are *vulnerable* .

CQ(f). **Which population is more affected? i.e., patients, doctors, administration, etc.**

To determine which of these groups experiences the most significant effects or consequences due to the vulnerabilities in RPM. The query below illustrates the scenario where it shows the Patient "`John`" and the medical device cause AdverseSideEffect in terms of LifeThreatening as shown in Figure 7.40.

SPARQL Query 9

```
SELECT ?Patient ?MedicalDevice ?AdverseSideEffect
WHERE {
    ?Patient :usingMedicalDevice ?MedicalDevice .
    ?MedicalDevice MIoT:mayCause ?AdverseSideEffect .
}
```

Patient	MedicalDevice	AdverseSideEffect
John	InfusionPump	LifeThreatening

Figure 7.40: The `Patient` are effected and cause `AdverseSideEffect`.

CQ(g). **Which type of data is more sensitive to vulnerabilities/attacks?**

In cybersecurity, various kinds of vulnerabilities occur and affect different types of data, such as personal, financial, or health data (i.e., vital sign, health condition, etc.,). Information about these different types of data and an analysis of their relative sensitivity are based on factors like potential impact, exploitability, and how frequently they are targeted in terms of CIA (Confidentiality, Integrity, and Availability). The following query shows the results in Figure 7.41 for these data types and their impact for CIA as CImpact (Confidentiality Impact), IImpact(Integrity Impact) and AImpact(Availability Impact).

SPARQL Query 8

```
SELECT ?DataType ?Vuln ?VulID ?PublishedDate ?AvailabilityImpact
?IntegrityImpact ?ConfidentialityImpact ?ExploitabilityScore
WHERE {
   ?Vuln a base:Vulnerability.
   ?Vuln base:vulnerabilityID ?VulID.
   ?Vuln base:hasPublished ?PublishedDate.
   {?Vuln base:hasAvailabilityImpact ?AvailabilityImpact.}
   {?Vuln base:hasIntegrityImpact ?IntegrityImpact.}
   {?Vuln base:hasConfidentialityImpact ?ConfidentialityImpact.}
   {?Vuln base:hasExploit ?e.}
   {?e base:hasExploitabilityScore ?ExploitabilityScore.}
   DataType a MIoT:MedicalDeviceFunction .
}
LIMIT 100
```

DataType	Vuln	PublishedDate	AImpact	IImpact	CImpact	ExploitabilityScore
HealthCondition	VulnerabilityCVE-2013-10027	2023-06-04T14:15Z	HIGH	HIGH	HIGH	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L
HealthCondition	VulnerabilityCVE-2019-11486	2019-04-23T22:29Z	HIGH	HIGH	HIGH	CVSS v3.1 Vector AV:L/AC:H/PR:L/UI:N/S:U/CH/I:H/A:H
HeartRate	VulnerabilityCVE-2021-28972	2021-03-22T17:15Z	HIGH	HIGH	HIGH	CVSS v2.0 Vector (AV:L/AC:L/Au:N/C:C/I:C/A:)
DeliverMedication	VulnerabilityCVE-2022-24859	2022-04-18T19:15Z	HIGH	NONE	NONE	CVSS v3.1 Vector AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Figure 7.41: `DataType` affected by vulnerabilities and impacts on *CIA*.

CQ(h). **What are the potential consequences and adverse side effects of identified vulnerabilities/ attacks?**

This framework is capable of identifying consequences/adverse side effects for detected vulnerabilities. The following query shows the adverse side effects for vulnerable medical devices.

SPARQL Query 10

```
SELECT ?MedicalDevice ?ASE
WHERE {
    ?ASE a MIoT:AdverseSideEffect .
    ?MedicalDevice MIoT:mayCause ?ASE .
}
```

MedicalDevice	AdverseSideEffect
InfusionPump	LifeThreatening
DeliverMedication	LifeThreatening

Figure 7.42: Medical devices shows the adverse side effects if these are vulnerable.

i. **What countermeasures should be implemented for specific vulnerabilities?** If the system encounter a vulnerability it will propose a countermeasures to mitigate those vulnerabilities. The following query shows the mitgations against vulnerability detection, the output is shown in Figure 7.43.

SPARQL Query 11

```
SELECT ?MedicalDevice ?ASE
WHERE {
    ?ASE a MIoT:AdverseSideEffect .
    ?MedicalDevice MIoT:mayCause ?ASE .
}
```

Mitigation	Vulnerability
SoftwareUpdateRecommendation	VulnerabilityCVE-2020-25668
SoftwareUpdateRecommendation	VulnerabilityCVE-2013-10027

Figure 7.43: `MedicalDevice` and its `AdverseSideEffect`

These various simple and complex queries can fulfil the requirements for competency questions (CQs) proposed for ontology modelling. With the help of these queries, one can identify specific vulnerabilities within medical devices, discuss their consequences, and assess their impact on patients. Additionally, this semantic framework is capable of recommending mitigation strategies if vulnerabilities or attacks are identified.

7.1.3 Evaluation of MIoT Semantic Model

7.1.3.1 Criteria-based Evaluation

Evaluation in ontology engineering refers to the process of assessing an ontology to ensure that it meets its intended goals, accurately represents the domain of knowledge it's designed for, and functions effectively within its intended context. This evaluation is crucial for ensuring the quality, performance, and usability of the ontology.

Numerous ontology evaluation methods have been proposed in the literature to determine whether an ontology accurately represents domain knowledge. After reviewing several common evaluation approaches, this approach employs a set of criteria to validate ontology design and content. This study chose a list of criteria from the criteria-based evaluation approaches [129; 249; 250], which include consistency, completeness, clarity, usability, applicability, and scalability. The MIoT ontology adequately covers all aspects of evaluation in ontology engineering including Consistency, Completeness, Clarity, Usability, Applicability and Scalability. The evaluation results confirmed the quality of the developed ontology in terms of the criteria-based evaluation approach, details are given below:

(a) ***Consistency:*** Checking for logical consistency within the ontology to ensure there are no contradictions in the definitions or relationships of concepts. Figure 7.44 shows the consistency through the Pellet Reasoner. Figure 6 shows the metric of ontology before and after the reasoning performed.

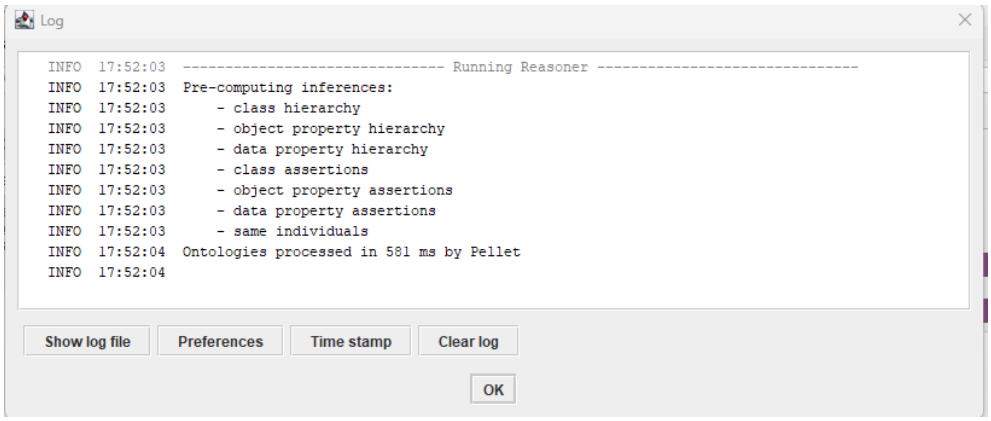
Log
INFO 17:52:03 ---------- Running Reasoner ----------
INFO 17:52:03 Pre-computing inferences:
INFO 17:52:03 - class hierarchy
INFO 17:52:03 - object property hierarchy
INFO 17:52:03 - data property hierarchy
INFO 17:52:03 - class assertions
INFO 17:52:03 - object property assertions
INFO 17:52:03 - data property assertions
INFO 17:52:03 - same individuals
INFO 17:52:04 Ontologies processed in 581 ms by Pellet
INFO 17:52:04
Show log file
Preferences
Time stamp
Clear log
OK

Figure 7.44: Consistency checking in Pellet Reasoner .

(b) ***Clarity:*** Clarity assesses how well an ontology conveys the intended meaning of its defined terms. The names and definitions of concepts must be unambiguous. Achieving clarity in the MIoT ontology involves assigning an unambiguous label or description to each class using methods such as "rdfs:label" or "rdfs:comment," as shown in Figure 7.45, where the concept "Product" has an annotation assigned as "rdfs:comment."

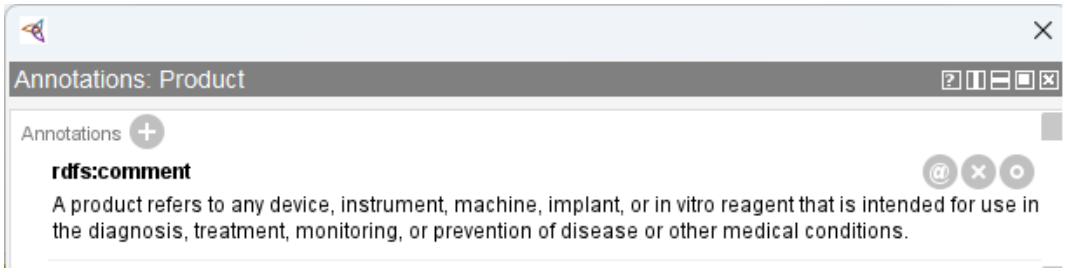
Annotations: Product
Annotations
rdfs:comment
A product refers to any device, instrument, machine, implant, or in vitro reagent that is intended for use in the diagnosis, treatment, monitoring, or prevention of disease or other medical conditions.

Figure 7.45: rdfs:comment for Concept `Product` .

(c) ***Completeness:*** Ensuring that the ontology adequately covers all relevant aspects of the domain it represents. This involves verifying that all necessary concepts, attributes, and relationships are included. Figures 7.46, 7.47, 7.48 show the examples of all those entities that are relevant to the domain of research. The completeness evaluated by CQs of ontology development that shows the MIoT ontology fulfills the requirement for completeness.

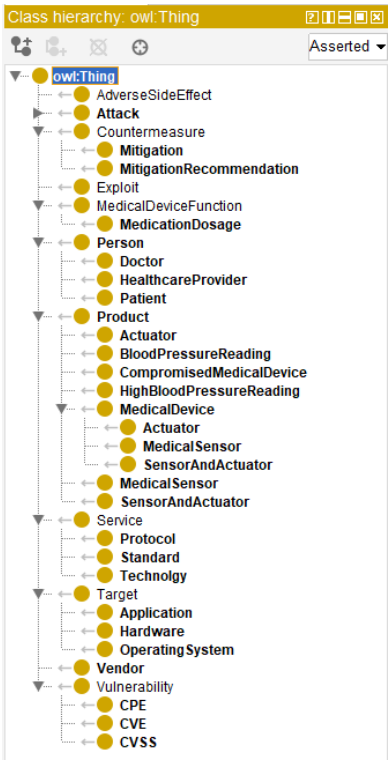

Figure 7.46: The hierarchical *Concepts* in MIoT Ontology.

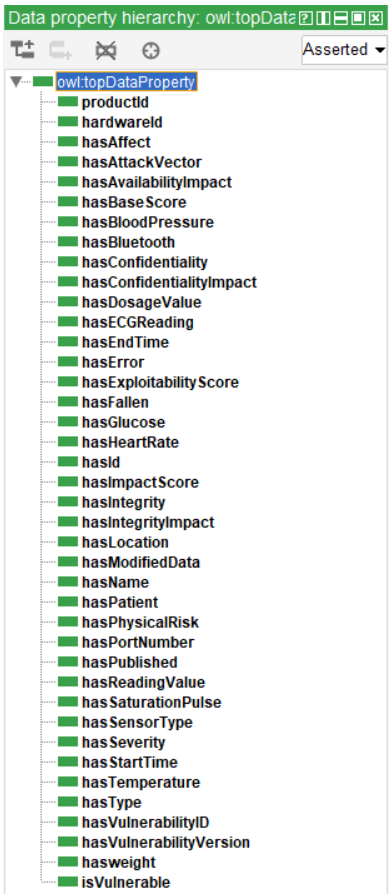

Figure 7.47: List of *Object Properties* for MIoT Ontology.

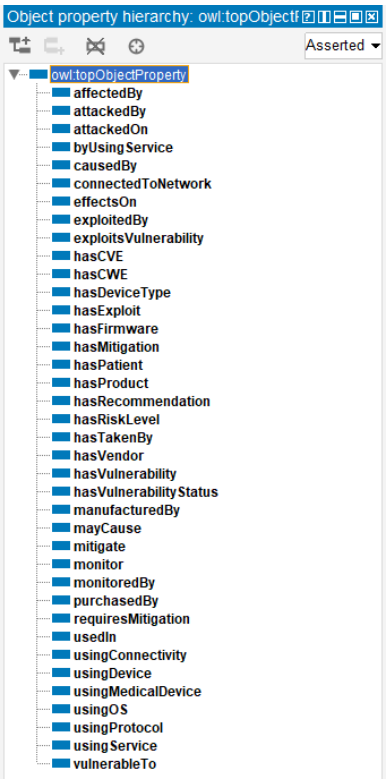

Figure 7.48: List of *Data Properties* for MIoT Ontology.

(d) ***Usability:*** Evaluating how effectively the ontology can be used in its intended applications. This includes assessing its integration with other systems and its performance in specific tasks, such as querying or reasoning. This section serves as a proof of conceptualization for the integration of a semantic model and a reasoning engine. The reasoning engine parses and stores explicit

facts, then uses these to infer new implicit facts. In this work, the reasoning engine Pellet operates based on the knowledge stored in the ontology and tries to find the vulnerabilities and compromised devices hidden within that knowledge. Pellet uses the tableaux algorithm to decide the satisfiability and consistency of ontologies by supporting forward chaining.

The MIoT ontology performed reasoning on the ruleset to infer new facts from existing knowledge, and external CVE information from the NVD dataset. An example is shown in Figure 7.49. This complex figure displays various instances from CVE that are related to the instance of MedicalSensor, such as a pacemaker.

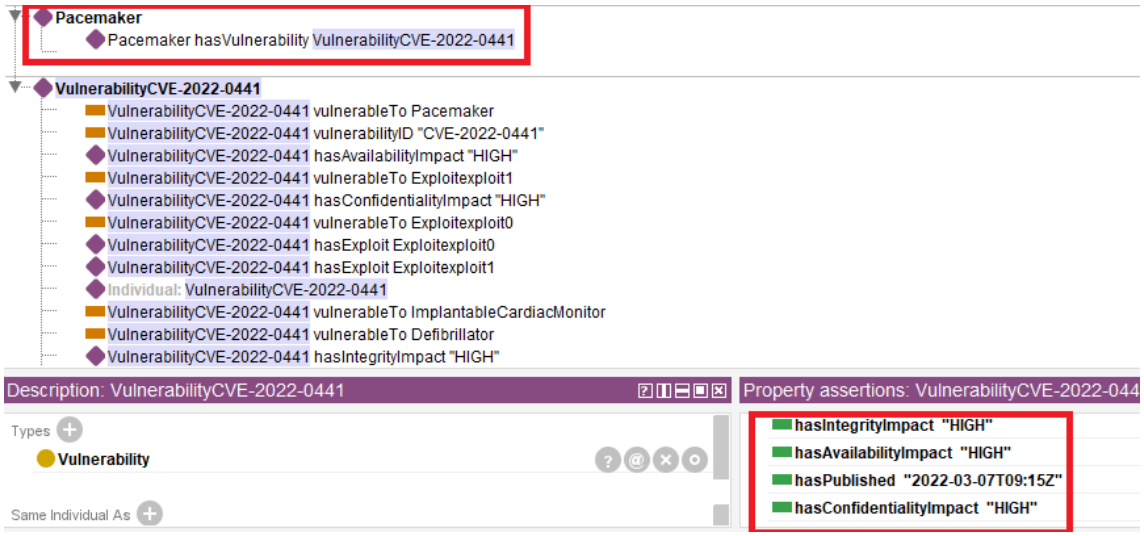

Figure 7.49: The Individual `Pacemaker` and related Vulnerabilities .

(e) ***Scalability:*** Scalability is the characteristic that Assess whether the ontology can handle growth in terms of size (more concepts, relationships) and complexity (more detailed knowledge representation) without losing performance. In this regard, the MIoT ontology is capable of being enhanced and acquiring more concepts and properties related to IoMT and the Cybersecurity domain. For example, the Concept Product and MedicalDevice can be used to add more subClasses related to clinical or hospital-based medical devices and use the same properties such as hasDeviceType, and hasProduct defined for medical devices used in MIoT ontology, particularly for remote patient monitoring. Similarly, the concept CPE subclass of Vulnerability can be used to address the information within CPE. The semantic framework's scalability is demonstrated through experiments that showed its ability to handle larger datasets such as live data streams from the NVD.

(f) ***Coherence:*** Checking the ontology for conceptual clarity and internal logical structure. Coherence ensures that the ontology makes sense as a whole and that its parts fit together in a meaningful way (*The conceptual model is presented in Chapter 4.*).

(g) ***Applicability:*** Assessing the ontology's relevance and utility for the specific problems or use cases it was designed to address. The MIoT ontology is validated on various use cases (in Chapter 4, Section 4.5.3) and with the existing framework (in Section 7.1.4 Validation of

Semantic Framework). This validation shows the applicability of MIoT ontology for the domain of IoMT and cybersecurity.

7.1.3.2 Generative AI-based Model Evaluation

Generative AI models learn patterns, structures, and relationships within input data and use this knowledge to create new, possible instances of data. This study utilizes generative AI models to evaluate the performance of rules developed to enhance security automation in the IoMT environment. These models are trained on provided rules and test use cases (Chapter 4, Case Study), enabling them to identify deviations from the norm and flag potential anomalies, vulnerabilities, and attacks. To train the model, the prompt is given to ChatGPT 4.0, which is provided here:

i. Prompt for ChatGPT 4.0

Here is a rule in quotes for vulnerability detection in the Internet of Medical Things with the expected inputs and the outputs, and the second row provides its explanation. Your task is to generate some tests that evaluate this rule for different inputs and also for any two different use cases provided below.

```
"BloodPressureReading(?r), vulnerableTo(?d, ?vuln), MedicalDevice(?d),
hasReadingValue(?r, ?reading), greaterThan(?reading, 120)
-> HighBloodPressureReading(?r)"
```

This rule states that if a medical device (denoted as 'd') is vulnerable to a certain vulnerability ('vuln'), and a blood pressure reading (denoted as 'r') is recorded such that the reading exceeds 120, it is inferred to be a high blood pressure reading.

Use Cases

(a) Medical devices for remote patient monitoring systems from a vendor utilize network connectivity to transmit data to healthcare providers.

(b) Due to an attack, data are modified and transmitted between the medical device and the healthcare provider through the network layer, compromising the confidentiality and integrity of the patient's information.

(c) Vulnerabilities in the network layer of remote patient monitoring systems may lead to inaccurate readings or manipulation of medical data.

(d) The compromise of medical devices, such as infusion pumps, due to vulnerabilities in their network layer, can have severe consequences, including adverse side effects for patients and the need for hospitalization to address medication-related issues.

(e) The incident with John's infusion pump underlines the importance of implementing robust security measures in remote patient monitoring systems to safeguard against potential attacks and vulnerabilities that could risk patient safety and compromise the accuracy of medical data.

ii. Evaluation Process by ChatGPT 4.0

To demonstrate the evaluation conducted by ChatGPT 4.0, the following steps were undertaken:

(a) **Input Preparation:** The provided rule and use cases were formatted as inputs to be processed by ChatGPT 4.0.

(b) **Model Training:** ChatGPT 4.0 was trained on these inputs, enabling the model to learn the patterns and structures necessary to identify potential vulnerabilities and anomalies.

(c) **Evaluation Execution:** ChatGPT 4.0 generated test cases based on the rule and use cases, systematically evaluating each scenario to detect deviations from expected behavior.

(d) **Result Generation:** The results of the evaluation, including identified anomalies and vulnerabilities, were recorded. ChatGPT 4.0 flagged instances where the rule correctly identified high blood pressure readings and noted any deviations.

(e) **Performance Assessment:** The performance and accuracy of the ruleset were assessed using a confusion matrix, which was calculated and presented alongside the results.

The generative AI model is trained based on these inputs to generate the results. This prompt is used for each rule, and results are obtained after learn the patterns provided, and identify potential anomalies and vulnerabilities. The following tables present the results after training the generative AI model. To assess the performance and accuracy of the proposed rules, a confusion matrix has also been calculated and is shown with each rule.

iii. Result Generation and Performance Assessment

(a) **Rule 1:** Table 7.13 shows the test results for HighBloodPressureReading and Table 7.14 shows the confusion matrix for the Rule 1.

```
BloodPressureReading(?r), vulnerableTo(?d, ?vuln), MedicalDevice(?d),
hasReadingValue(?r, ?eading), greaterThan(?reading, 120)
-> HighBloodPressureReading(?r)
```

Metrics Calculation

(a) Accuracy

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} = \frac{3+2}{3+2+1+0} = \frac{5}{6} \approx 0.833 \tag{7.1}$$

(b) Precision:

$$\text{Precision} = \frac{TP}{TP + FP} = \frac{3}{3+1} = \frac{3}{4} = 0.75 \tag{7.2}$$

Table 7.13: Rule 1: Test Results for HighBloodPressureReading Detection

Test Case	Device ID	Vuln	Reading Value	Expected Output	Actual Output
1	Device1	Vuln1	130	HighBloodPressureReading	HighBloodPressureReading
2	Device1	Vuln1	110	Not HighBloodPressureReading	Not HighBloodPressureReading
3	Device2	Vuln2	140	HighBloodPressureReading	HighBloodPressureReading
4	Device2	Vuln2	100	Not HighBloodPressureReading	Not HighBloodPressureReading
5	Infusion Pump1	Vuln3	150	HighBloodPressureReading	HighBloodPressureReading
6	Infusion Pump1	Vuln3	90	Not HighBloodPressureReading	Not HighBloodPressureReading

Table 7.14: Confusion Matrix for *Rule 1:* HighBloodPressureReading Detection

	Predicted HighBPReading	**Predicted Not HighBPReading**
Actual HighBPReading	TP = 3	FN = 0
Actual Not HighBPReading	FP = 1	TN = 2

(c) Recall:

$$\text{Recall} = \frac{TP}{TP + FN} = \frac{3}{3 + 0} = 1.0 \tag{7.3}$$

(d) F1 Score:

$$\text{F1 Score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} = 2 \times \frac{0.75 \times 1.0}{0.75 + 1.0} = 2 \times \frac{0.75}{1.75} \approx 0.857 \tag{7.4}$$

Summary of Metrics

- **Accuracy:** 0.833
- **Precision:** 0.75
- **Recall:** 1.0
- **F1 Score:** 0.857

These metrics indicate that the rule performs well in terms of correctly identifying high blood pressure readings from vulnerable medical devices, with high recall and a good balance between precision and recall as indicated by the F1 score.

(b) **Rule 2:** Table 7.15 shows the test results for CompromisedMedicalDevices (CMD) along with the confusion matrix shown in Table 7.29

```
MedicalDevice(?d), connectedToNetwork(?d, ?networklayer),
hasModifiedData(?d, true), hasVulnerability(?d, ?vuln)
-> CompromisedMedicalDevice(?d)
```

Metrics Calculation

Table 7.15: Rule 2: Test Results for CompromisedMedicalDevice Detection (CMD)

Test Case	Device ID	Network Layer	Modified Data	Vuln	Expected Output	Actual Output
1	Device1	Network1	true	Vuln1	CMD	CMD
2	Device1	Network1	false	Vuln1	Not CMD	Not CMD
3	Device2	Network2	true	Vuln2	CMD	CMD
4	Device2	Network2	true	None	Not CMD	Not CMD
5	Infusion Pump1	Network3	true	Vuln3	CMD	CMD
6	Infusion Pump1	Network3	false	Vuln3	Not CMD	Not CMD

Table 7.16: Confusion Matrix for *Rule 2:* CompromisedMedicalDevice Detection

	Predicted Compromised	**Predicted Not Compromised**
Actual Compromised	TP = 3	FN = 1
Actual Not Compromised	FP = 0	TN = 2

(a) Accuracy

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} = \frac{3 + 2}{3 + 2 + 0 + 1} = \frac{5}{6} \approx 0.833 \tag{7.5}$$

(b) Precision

$$\text{Precision} = \frac{TP}{TP + FP} = \frac{3}{3 + 0} = 1.0 \tag{7.6}$$

(c) Recall

$$\text{Recall} = \frac{TP}{TP + FN} = \frac{3}{3 + 1} = \frac{3}{4} = 0.75 \tag{7.7}$$

(d) F1 Score

$$\text{F1 Score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} = 2 \times \frac{1.0 \times 0.75}{1.0 + 0.75} = 2 \times \frac{0.75}{1.75} \approx 0.857 \tag{7.8}$$

Summary of Metrics

- **Accuracy:** 0.833
- **Precision:** 1.0
- **Recall:** 0.75
- **F1 Score:** 0.857

The rule is tested across different scenarios to ensure it correctly identifies compromised medical devices based on network connectivity, data modification, and device vulnerabilities. The confusion matrix helps evaluate the rule's accuracy by showing the number of true positives, false positives, true negatives, and false negatives. The use cases provide context to understand the implications of the rule in real-world situations. The results are good, particularly in terms of precision, but there is room for improvement in recall. Given the critical nature of detecting compromised medical devices, efforts should be made to improve the rule to catch more compromised devices (higher recall) while maintaining or minimally affecting precision.

(c) **Rule 3:** Table 7.17 shows the test results for AdverseSideEffect and Table 7.32 shows the confusion matrix.

```
Patient(?p), usingMedicalDevice(?p, ?d), greaterThan(?dosage, 10)
-> AdverseSideEffect(?p)
```

Table 7.17: Rule 3: Test Results for Adverse Side Effects Detection

Test Case	Patient ID	Medical Device	Dosage	Expected Output	Actual Output
1	Patient1	Device1	15	AdverseSideEffect	AdverseSideEffect
2	Patient1	Device1	8	Not AdverseSideEffect	Not AdverseSideEffect
3	Patient2	Device2	12	AdverseSideEffect	AdverseSideEffect
4	Patient2	Device2	5	Not AdverseSideEffect	Not AdverseSideEffect
5	Patient3	Device3	20	AdverseSideEffect	AdverseSideEffect
6	Patient3	Device3	7	Not AdverseSideEffect	Not AdverseSideEffect

Table 7.18: Confusion Matrix for *Rule 3:* AdvereSideEffect Detection

	Predicted AdverseSideEffect	**Predicted Not AdverseSideEffect**
Actual AdverseSideEffect	TP = 3	FN = 0
Actual Not AdverseSideEffect	FP = 0	TN = 3

Metrics Calculation

(a) Accuracy

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} = \frac{3+3}{3+3+0+0} = \frac{6}{6} = 1.0 \tag{7.9}$$

(b) Precision

$$\text{Precision} = \frac{TP}{TP + FP} = \frac{3}{3+0} = 1.0 \tag{7.10}$$

(c) Recall

$$\text{Recall} = \frac{TP}{TP + FN} = \frac{3}{3+0} = 1.0 \tag{7.11}$$

(d) F1 Score

$$\text{F1 Score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} = 2 \times \frac{1.0 \times 1.0}{1.0 + 1.0} = 2 \times \frac{1.0}{2.0} = 1.0 \tag{7.12}$$

Summary of Metrics

- **Accuracy:** 1.0
- **Precision:** 1.0
- **Recall:** 1.0
- **F1 Score:** 1.0

The results are excellent across all metrics. With perfect scores in accuracy, precision, recall, and F1 score, the rule is highly effective at correctly identifying patients who may experience adverse side effects based on their dosage levels. This indicates that the rule is both reliable and accurate in this context. These metrics and the perfect confusion matrix imply that the rule performs exceptionally well for the given test cases, effectively identifying all true positives and true negatives without any false positives or false negatives.

(d) **Rule 4:** Table 7.19 shows the test results for Vulnerability and Exploit detection. Table 7.20 shows the confusion matrix for the acquired results.

```
Vulnerability(?vuln), Exploit(?exploit) ->
vulnerableTo(?vuln, ?exploit)
```

Table 7.19: Rule 4: Test Results for Vulnerability and Exploit Detection

Test Case	Vuln ID	Exploit ID	Expected Output	Actual Output
1	Vuln1	Exploit1	vulnerableTo(Vuln1, Exploit1)	vulnerableTo(Vuln1, Exploit1)
2	Vuln1	Exploit2	vulnerableTo(Vuln1, Exploit2)	vulnerableTo(Vuln1, Exploit2)
3	Vuln2	Exploit1	vulnerableTo(Vuln2, Exploit1)	vulnerableTo(Vuln2, Exploit1)
4	Vuln2	None	Not vulnerableTo(Vuln2, Exploit1)	Not vulnerableTo(Vuln2, Exploit1)
5	Vuln3	Exploit3	vulnerableTo(Vuln3, Exploit3)	vulnerableTo(Vuln3, Exploit3)
6	Vuln3	Exploit1	vulnerableTo(Vuln3, Exploit1)	vulnerableTo(Vuln3, Exploit1)

Table 7.20: Confusion Matrix for *Rule 4:* Vulnerability and Exploit Detection

	Predicted VulnerableTo	**Predicted Not VulnerableTo**
Actual VulnerableTo	TP = 4	FN = 1
Actual Not VulnerableTo	FP = 0	TN = 1

Metrics Calculation

(a) Accuracy

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} = \frac{4 + 1}{4 + 1 + 0 + 1} = \frac{5}{6} \approx 0.833 \tag{7.13}$$

(b) Precision

$$\text{Precision} = \frac{TP}{TP + FP} = \frac{4}{4 + 0} = 1.0 \tag{7.14}$$

(c) Recall

$$\text{Recall} = \frac{TP}{TP + FN} = \frac{4}{4 + 1} = \frac{4}{5} = 0.8 \tag{7.15}$$

(d) F1 Score

$$\text{F1 Score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} = 2 \times \frac{1.0 \times 0.8}{1.0 + 0.8} = 2 \times \frac{0.8}{1.8} \approx 0.889 \tag{7.16}$$

Summary of Metrics

- **Accuracy:** 0.833
- **Precision:** 1.0
- **Recall:** 0.8
- **F1 Score:** 0.889

The results indicate that the rule is effective at identifying vulnerabilities that are susceptible to exploits. While the precision is perfect, indicating no false positives, the recall could be improved to ensure that more vulnerabilities are detected. This is crucial in the context of medical devices, where undetected vulnerabilities could lead to severe consequences. Overall, the rule performs well, but further refinement could enhance its recall and overall effectiveness.

(e) **Rule 5:** Table 7.21 presents the test results for vulnerability, exploit, and attack detection, while Table 7.22 displays the confusion matrix.

```
Vulnerability(?vuln), Exploit(?exploit),
exploitedBy(?vuln, ?attack) -> vulnerableTo(?vuln, ?attack)
```

Table 7.21: Rule 5: Test Results for Vulnerability, Exploit, and Attack Detection

Test Case	Vuln ID	Exploit ID	Attack ID	Expected Output	Actual Output
1	Vuln1	Exploit1	Attack1	vulnerableTo(Vuln1, Attack1)	vulnerableTo(Vuln1, Attack1)
2	Vuln1	Exploit1	Attack2	Not vulnerableTo(Vuln1, Attack2)	Not vulnerableTo(Vuln1, Attack2)
3	Vuln2	Exploit2	Attack1	vulnerableTo(Vuln2, Attack1)	vulnerableTo(Vuln2, Attack1)
4	Vuln2	None	Attack3	Not vulnerableTo(Vuln2, Attack3)	Not vulnerableTo(Vuln2, Attack3)
5	Vuln3	Exploit3	Attack2	vulnerableTo(Vuln3, Attack2)	vulnerableTo(Vuln3, Attack2)
6	Vuln3	Exploit1	Attack3	vulnerableTo(Vuln3, Attack3)	vulnerableTo(Vuln3, Attack3)

Table 7.22: Confusion Matrix for Rule 5: Vulnerability, Exploit and Attack Detection

	Predicted VulnerableTo	Predicted Not VulnerableTo
Actual VulnerableTo	TP = 4	FN = 0
Actual Not VulnerableTo	FP = 0	TN = 2

Metrics Calculation

(a) Accuracy

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} = \frac{4 + 2}{4 + 2 + 0 + 0} = \frac{6}{6} = 1.0 \tag{7.17}$$

(b) Precision

$$\text{Precision} = \frac{TP}{TP + FP} = \frac{4}{4 + 0} = 1.0 \tag{7.18}$$

(c) Recall

$$\text{Recall} = \frac{TP}{TP + FN} = \frac{4}{4 + 0} = 1.0 \tag{7.19}$$

(d) F1 Score

$$\text{F1 Score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} = 2 \times \frac{1.0 \times 1.0}{1.0 + 1.0} = 2 \times \frac{1.0}{2.0} = 1.0 \tag{7.20}$$

Summary of Metrics

- **Accuracy:** 1.0
- **Precision:** 1.0
- **Recall:** 1.0
- **F1 Score:** 1.0

The rule performs perfectly in identifying vulnerabilities that are susceptible to attacks, with perfect precision, recall, and F1 score. This indicates that the rule is both reliable and accurate in this context. Given the critical nature of vulnerability detection in medical devices, this high performance is crucial for ensuring the security and safety of medical systems.

(f) **Rule 6:** Table 7.23 presents the test results for medical device attack risk, while Table 7.24 displays the confusion matrix.

```
MedicalDevice(?d), hasSeverity(?d, "high")
-> AttackRisk(?d), hasRiskLevel(?d, HighRisk)
```

Metrics Calculation

(a) Accuracy

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} = \frac{3 + 3}{3 + 3 + 0 + 0} = \frac{6}{6} = 1.0 \tag{7.21}$$

(b) Precision

$$\text{Precision} = \frac{TP}{TP + FP} = \frac{3}{3 + 0} = 1.0 \tag{7.22}$$

Table 7.23: Rule 6: Test Results for Medical Device Attack Risk Detection

Test Case	Medical Device	Severity	Expected Output	Actual Output
1	Device1	high	AttackRisk(Device1), HighRisk	AttackRisk(Device1), HighRisk
2	Device1	low	Not AttackRisk(Device1), Not HighRisk	Not AttackRisk(Device1), Not HighRisk
3	Device2	high	AttackRisk(Device2), HighRisk	AttackRisk(Device2), HighRisk
4	Device2	medium	Not AttackRisk(Device2), Not HighRisk	Not AttackRisk(Device2), Not HighRisk
5	Device3	high	AttackRisk(Device3), HighRisk	AttackRisk(Device3), HighRisk
6	Device3	low	Not AttackRisk(Device3), Not HighRisk	Not AttackRisk(Device3), Not HighRisk

Table 7.24: Confusion Matrix for *Rule 6:* Medical Device Attack Risk detection

	Predicted AttackRisk	**Predicted Not AttackRisk**
Actual HighRisk	TP = 3	FN = 0
Actual Not HighRisk	FP = 0	TN = 3

(c) Recall

$$\text{Recall} = \frac{TP}{TP + FN} = \frac{3}{3 + 0} = 1.0 \tag{7.23}$$

(d) F1 Score

$$\text{F1 Score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} = 2 \times \frac{1.0 \times 1.0}{1.0 + 1.0} = 2 \times \frac{1.0}{2.0} = 1.0 \tag{7.24}$$

Summary of Metrics

- **Accuracy:** 1.0
- **Precision:** 1.0
- **Recall:** 1.0
- **F1 Score:** 1.0

The rule performs perfectly in identifying medical devices with high-risk vulnerabilities based on their severity, with perfect precision, recall, and F1 score. This indicates that the rule is both reliable and accurate in this context. Given the critical nature of risk assessment in medical devices, this high performance is crucial for ensuring the security and safety of medical systems.

(g) **Rule 7:** Table 7.25 shows the test results for Mitigation recommendation and Table 7.26 shows the confusion matrix for the Rule 7.

```
Vulnerability(?vuln), hasRecommendation(?vuln, ?mitigation)
-> MitigationRecommendation(?mitigation)
```

Table 7.25: Rule 7: Test Results for Mitigation Recommendations (MR)

Test Case	Vuln ID	Recommendation	Expected Output	Actual Output
1	Vuln1	PatchUpdate	MR (PatchUpdate)	MR (PatchUpdate)
2	Vuln1	NetworkIsolation	MR (NetworkIsolation)	MR (NetworkIsolation)
3	Vuln2	FirmwareUpgrade	MR (FirmwareUpgrade)	MR (FirmwareUpgrade)
4	Vuln2	None	Not MR (None)	Not MR (None)
5	Vuln3	StrongAuthentication	MR (StrongAuthentication)	MR (StrongAuthentication)
6	Vuln3	Encryption	MR (Encryption)	MR (Encryption)

Table 7.26: Confusion Matrix for *Rule 7:* Mitigation Recommendation (MR)

	Predicted MR	**Predicted Not MR**
Actual MitigationRecommendation	TP = 4	FN = 1
Actual Not MitigationRecommendation	FP = 0	TN = 1

Metrics Calculation

(a) Accuracy

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} = \frac{4 + 1}{4 + 1 + 0 + 1} = \frac{5}{6} \approx 0.833 \tag{7.25}$$

(b) Precision

$$\text{Precision} = \frac{TP}{TP + FP} = \frac{4}{4 + 0} = 1.0 \tag{7.26}$$

(c) Recall

$$\text{Recall} = \frac{TP}{TP + FN} = \frac{4}{4 + 1} = \frac{4}{5} = 0.8 \tag{7.27}$$

(d) F1 Score

$$\text{F1 Score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} = 2 \times \frac{1.0 \times 0.8}{1.0 + 0.8} = 2 \times \frac{0.8}{1.8} \approx 0.889 \tag{7.28}$$

Summary of Metrics

- **Accuracy:** 0.833
- **Precision:** 1.0
- **Recall:** 0.8
- **F1 Score:** 0.889

While an accuracy of 0.833 may seem high, it doesn't always reflect performance, especially with imbalanced data or differing costs for false positives and negatives. The F1 score of 0.889 is more informative as it balances precision and recall. Since the F1 score is higher, it better represents the model's classification ability and should be prioritized when assessing performance.

Overall, the rule performs well in identifying mitigation recommendations for vulnerabilities, with perfect precision and a strong F1 score. However, there is room for improvement in recall

to ensure that more recommendations are identified. Given the critical nature of mitigation in medical devices, enhancing recall would be beneficial to ensure comprehensive security measures.

(h) **Rule 8:** Table 7.27 displays the test results for Mitigation Recommendation (MR) based on Risk level and Table 7.28 provides the confusion matrix.

```
MedicalDevice(?d), hasRiskLevel(?d, ?m)
-> MitigationRecommendation(?d)
```

Table 7.27: Rule 8: Test Results for Mitigation Recommendations Based on Risk Levels

Test Case	Medical Device	Risk Level	Expected Output	Actual Output
1	Device1	High	MR (Device1)	MR (Device1)
2	Device1	Medium	MR (Device1)	MR (Device1)
3	Device2	Low	MR (Device2)	MR (Device2)
4	Device2	None	Not MR (Device2)	Not MR (Device2)
5	Device3	Critical	MR (Device3)	MR (Device3)
6	Device3	None	Not MR (Device3)	Not MR (Device3)

Table 7.28: Confusion Matrix for *Rule 8:* Mitigation Recommendation (MR) based on Risk Level

	Predicted MR	**Predicted Not MR**
Actual MitigationRecommendation	TP = 4	FN = 0
Actual Not MitigationRecommendation	FP = 0	TN = 2

Metrics Calculation

(a) Accuracy

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} = \frac{4 + 2}{4 + 2 + 0 + 0} = \frac{6}{6} = 1.0 \tag{7.29}$$

(b) Precision

$$\text{Precision} = \frac{TP}{TP + FP} = \frac{4}{4 + 0} = 1.0 \tag{7.30}$$

(c) Recall

$$\text{Recall} = \frac{TP}{TP + FN} = \frac{4}{4 + 0} = 1.0 \tag{7.31}$$

(d) F1 Score

$$\text{F1 Score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} = 2 \times \frac{1.0 \times 1.0}{1.0 + 1.0} = 2 \times \frac{1.0}{2.0} = 1.0 \tag{7.32}$$

Summary of Metrics

- **Accuracy:** 1.0
- **Precision:** 1.0
- **Recall:** 1.0
- **F1 Score:** 1.0

The rule performs perfectly in identifying medical devices that need mitigation recommendations based on their risk levels, with perfect precision, recall, and F1 score. This indicates that the rule is both reliable and accurate in this context. Given the critical nature of mitigation in medical devices, this high performance is crucial for ensuring the security and safety of medical systems.

iv. Summary of Ruleset Evaluation via Generative AI Model:

Overall, the rules demonstrate high effectiveness in identifying vulnerabilities, exploits, attacks, and anomalies within the IoMT environment. The high precision across all rules ensures that the identified issues are valid, thereby minimizing false alarms. Although two of the rules exhibit slightly lower recall due to false negatives, the overall performance remains robust, with excellent accuracy and F1 scores. These rules are reliable for use in the IoMT environment; however, real-time data and more complex scenarios are needed to further enhance recall and ensure comprehensive vulnerability detection.

7.1.4 Validation of the MIoT Semantic Framework

To validate the performance of the semantic framework, this study compares and evaluates the MIoT semantic framework with the existing IoMT-SAF framework [160]. IoMT-SAF is a Python web application designed to evaluate the security of IoMT solutions, offering two modules: the Recommendation Assessment Module and the IoMT Security Assessment Framework. The developed framework, using an ontological scenario-based approach, ensures specific solutions can be adapted based on real-world scenarios. IoMT-SAF classifies IoMT security threats and recommends corresponding security controls.

Primarily utilized by solution providers, IoMT-SAF enables the assessment and recommendation of security in products. The recommendation module uses an ontological approach to identify IoMT security threats based on specific scenarios and recommend appropriate countermeasures, while the assessment module allows stakeholders to evaluate the degree of security in their chosen IoMT solutions. The authors claim IoMT-SAF utilizes ontology and context-aware rules for reasoning and recommendation. However, they did not explain the ontology development and ruleset generation or discuss the reasoning mechanism. Evaluations were performed based on two kinds of experiments: expert-based evaluation and vulnerability-based evaluation. In the expert-based evaluation, 7 graduate students from the cybersecurity domain were chosen to evaluate the performance of the framework.

In the vulnerability-based evaluation, the authors used the NVD database. Through analysis, 40 distinct vulnerabilities related to IoMT, healthcare, medical, etc., were identified from the NVD CVE, categorizing them under 11 scenarios based on stakeholders, solution type, and architecture. IoMT-SAF highlights security issues, recommends necessary security attributes, and addresses confusion among stakeholders regarding security measures for those 11 scenarios.

This work briefly touches on the complexity of existing IoMT solutions, and the assessment framework may not fully address the dynamic nature of evolving IoT technology. Additional research is needed to validate the framework's effectiveness across various IoMT systems and compare it with existing security standards.

In contrast, this study emphasizes the importance of security in the evolving landscape of IoMT cybersecurity, tackling the challenge posed by traditional security measures that struggle with complex vulnerabilities. It presents a comprehensive semantic framework for vulnerability detection in IoMT systems, consisting of two core components: a semantic model and a knowledge graph. The semantic model features a novel MIoT ontology by following knowledge engineering and structured life cycle methodologies and employs de-facto standards such as RDF formalism to enrich data annotation and facilitate knowledge base development. The framework analyzes data, detects vulnerabilities, and generates a knowledge graph that stores Cyber Threat Intelligence (CTI) and supports visualization. Its effectiveness is assessed through complex queries and a Generative AI model and validated through the existing framework. The details of the comparison between IoMT-SAF and the MIoT Semantic Framework are given below based on a few proposed criteria as shown in Table 7.29.

Table 7.29: Comparison of MIoT Semantic Framework and IoMT-SAF

Comparison of MIoT Semantic Framework and IoMT-SAF						
Framework	**Domain of Research**	**Semantic Model**	**Reasoning Capability**	**Knowledge Graph Representation**	**Query Interface**	**Evaluation and Validation**
MIoT Semantic Framework	IoMT/RPM and Vulnerability Detection	Yes	Yes	Ruleset Generation with de-facto standards	Yes	Evaluation (Ontology Engineering practices and Gen AI Model based). Validation through IoMT-SAF framework
IoMT-SAF	IoMT and Vulnerability Detection	Ontology development	Context-aware rules (Descriptive)	No	No	Vulnerability-based Evaluation Expert-Based Evaluation

(a) **Domain of Research**

Both studies address the IoMT (Internet of Medical Things) and cybersecurity domains. While IoMT-SAF provides a general focus on IoMT, this study specifically examines medical devices used in remote patient monitoring settings. These devices transfer data to doctors or healthcare providers for diagnosis, assessment, and treatment. Due to vulnerabilities in the network layer,

these medical devices connected via Bluetooth, Wi-Fi, or cloud-based systems are particularly susceptible to cyberattacks.

(b) **Semantic Modelling**

IoMT-SAF constructs an ontology that defines concepts, relationships, instances, and axioms representing key elements such as stakeholders, solutions, and architectures. These elements demonstrate specific scenarios related to particular medical devices and their security attributes. However, the study lacks context regarding semantic modeling in terms of interoperability, inference, machine readability, etc.

In contrast, the work presented in this study provides a semantic model containing a knowledge base and an inference engine. The knowledge base constitutes the domain ontology, facts, and ruleset. The domain ontology (i.e., MIoT ontology) is developed by following knowledge engineering methodologies, standards, and vocabularies. The MIoT ontology captures cybersecurity aspects in remote patient monitoring settings, defining vulnerabilities, exploits, and cyberattacks along with their adverse side effects for patients, impacts on medical devices, and recommended mitigations. This knowledge base is also integrated with the NVD dataset to obtain information about CVE and CVSS, capturing related vulnerabilities and their impacts, making the process more robust, efficient, and adoptable by the community. Additionally, the rule-based reasoning performed by the inference engine assesses the ruleset and discovers hidden facts from the knowledge base, allowing the system to detect new vulnerabilities that were not previously assigned to medical devices.

Additionally, this semantic model is responsible for logic-based reasoning to infer new facts from existing knowledge in the knowledge base. This automation capability informs doctors and healthcare providers about new vulnerabilities arising in the system, their influence on patients, and their impacts on medical devices.

(c) **Reasoning Capability**

SWRL is a powerful language for expressing rules in combination with OWL ontologies, and it has become a key component in semantic web applications. It is often used in conjunction with ontology reasoners and is considered a 'de-facto' standard derived from the Protege SWRLTab plugin. The semantic model proposed in the MIoT semantic framework offers reasoning capabilities where rules are triggered by the inference engine to discover new facts based on logic. This study details the reasoning approach in different steps, while there are no explicitly defined rules or discussions in the IoMT-SAF framework. Neither author describes the mechanism of the reasoning process in their work.

(d) **Knowledge Graph Representation**

Knowledge graphs emphasize the organization and representation of knowledge to facilitate more sophisticated forms of analysis and decision-making. A knowledge graph is a structured representation of knowledge, typically in the form of interconnected entities and relationships. The knowledge graph in the MIoT semantic framework provides a means for organizing and

navigating information for visualization and enabling advanced querying. The MIoT knowledge graph is particularly used for integrating disparate data sources (e.g., NVD data), capturing domain-specific knowledge (semantic model), and supporting complex querying (through a SPARQL endpoint). It provides alerts in the form of query output to healthcare providers in case of any vulnerability detection in the system.

(e) **Query Interface**

This study evaluates the semantic framework by applying the query mechanism to find insights into vulnerabilities, their impacts, and recommendations. These queries run on live NVD CVE data, allowing the system to be updated with new vulnerabilities. However, IoMT-SAF lacks this feature.

(f) **Evaluation and Validation**

In terms of evaluation and validation, this study showcases various approaches to evaluate the proposed work:

- At the Conceptual Level: The MIoT model is validated using verification and validation techniques [230; 231].
- At the Perception Level: The Knowledge Engineering approach is adopted, and a criteria-based approach [129; 249; 250] is used to evaluate the semantic model. Additionally, the innovative generative AI model represents a cutting-edge solution for automated reasoning over aggregated semantic knowledge, offering a revolutionary approach to testing the ruleset. This sophisticated technology leverages state-of-the-art algorithms to deliver groundbreaking performance and advanced capabilities, setting a new standard in the field.
- At the Practical Level: The MIoT semantic framework is validated against the existing IoMT-SAF framework [160]. The evaluation results demonstrate that the proposed MIoT semantic framework is highly effective in detecting vulnerabilities and anomalies, particularly within remote patient monitoring (RPM) settings, making it more applicable and reliable for these environments.

7.1.4.1 Summary of Key Differences

- **Scope and Capabilities:** IoMT-SAF primarily focuses on defining stakeholders and architecture, but it lacks in-depth semantic modeling. In contrast, the MIoT framework provides detailed semantic modeling and advanced reasoning capabilities.
- **Knowledge Base:** The MIoT semantic framework includes a standardized ontology integrated with external datasets, enabling comprehensive security management. This level of integration and standardization is not present in IoMT-SAF.
- **Inference:** MIoT features an inference engine that offers rule-based reasoning to uncover hidden vulnerabilities. IoMT-SAF does not include this capability.

- **Visualization Capabilities:** The MIoT semantic framework supports linked data visualization, where nodes (entities) are interconnected through edges that describe their relationships. This feature enhances understanding and analysis of the data.
- **Query Interface:** MIoT framework utilizes SPARQL, a powerful query language, to extract insights from the RDF knowledge graph, providing a robust interface for querying the database.

7.2 Summary of the Chapter

The chapter has presented the implementation, evaluation and validation of a comprehensive semantic framework for vulnerability detection in the Internet of Medical Things (IoMT), highlighting two core components: a semantic model and a visualization and query interface . The semantic model implements the MIoT ontology, generates rulesets, and performs reasoning using an inference engine to uncover hidden relationships and infer new facts. The knowledge graph stores data from the semantic model and integrates it with the NVD database via an API for visualization, allowing access through SPARQL queries to assess vulnerabilities.

The semantic model is rigorously evaluated using a standardized knowledge engineering methodology and validated with large language models, including generative AI models (i.e., ChatGPT 4o), to ensure the robustness of the semantic model. The entire semantic framework is further validated by comparing it with an existing framework, an established framework that employs IoMT components for identifying security issues and providing recommendations.

Chapter 8

Results and Findings

This chapter presents a comprehensive analysis of the research study's outcomes, focusing on the development of a semantic framework for enhancing the security of the Internet of Medical Things (IoMT). This chapter explores semantic modeling, automation, visualization, and querying techniques employed in the framework's development. Utilizing optimized methodologies, the performance of the semantic framework is evaluated and discussed in detail. It serves to clarify the key responses to the research questions speculated in this thesis. Through the following discussion, this chapter articulates the research journey, describing the path leading to the discovery of significant findings and insights.

8.1 Results

This study provides a comprehensive approach to addressing key challenges in healthcare technology such as interoperability, heterogeneity, scalability, integration, and visualization. In this regard, a semantic framework has been developed to provide interoperability by leveraging MIoT ontology and controlled vocabularies like schema.org, ensuring seamless communication and data exchange between various systems and medical devices. This interoperability enhances the compatibility and integration of different healthcare technologies, facilitating a cohesive ecosystem for sharing and utilizing health data. Medical devices, such as BP monitors and heart rate monitors, often come from different vendors with varying specifications and data formats. this solution is designed to handle this diversity and heterogeneity by enabling integration among medical devices from different manufacturers.

Furthermore, in terms of application and addressing Common Vulnerability Enumeration (CVE), Common Vulnerability Scoring System (CVSS), and similar security concerns, this solution can adapt to growing demands and evolving security vulnerabilities. It ensures robust protection and performance across various scenarios and scales by providing scalability. By integrating diverse sources of information such as the NVD database and using ontology-based knowledge representation, this solution improves the depth and accuracy of analysis and supports decision-making based on reasoning.

Finally, this solution prioritizes visualization through the knowledge graph. This visualization tool provides an intuitive and interactive representation of complex relationships and data structures within the healthcare domain. By visualizing interconnected concepts and entities, this solution

facilitates better understanding, analysis, and interpretation of healthcare data, ultimately empowering stakeholders to make informed decisions and drive meaningful outcomes. The key areas are discussed here:

8.1.1 Implementation of the Semantic Framework

This section elaborates on the comprehensive semantic framework designed for the Internet of Medical Things (IoMT) environment, specifically for Remote Patient Monitoring (RPM), which consists of two primary components:

8.1.1.1 Semantic Model

This component incorporates the MIoT ontology, generates rulesets, and performs reasoning using an inference engine. The semantic model uses semantic technologies, vocabularies, and standards to define entities and relationships through semantics and annotations. Automation is greatly enhanced by the semantic framework, which is adept at revealing hidden relationships within the data and inferring new facts that were not explicitly stated. This functionality is crucial for identifying complex patterns and anomalies in the IoMT environment. Automation reduces the burden on human analysts, allowing them to focus on more complex and high-priority issues. Furthermore, automated systems can operate continuously, providing real-time monitoring and response capabilities that are crucial for maintaining security in a dynamic IoMT environment such as healthcare.

Evaluation of the Semantic Model

The semantic model underwent a rigorous evaluation using a standardized criteria-based approach and large language models, including generative AI models. The criteria-based approach demonstrated that the MIoT semantic model meets its intended goals, accurately represents the domain of knowledge it is designed for, and functions effectively within its intended context. This evaluation confirmed the quality and performance of the MIoT ontology in terms of consistency, completeness, clarity, usability, coherence, applicability, and scalability.

Evaluation using the generative AI model focused on several key metrics, including accuracy, precision, recall, and F1 score, to assess the performance of the ruleset designed for vulnerability detection. These evaluations provided comprehensive insights into the effectiveness and reliability of the semantic model in identifying and managing vulnerabilities within the IoMT environment.

However, generative AI is a young field, making it essential to verify the results produced by these models to ensure they are both comparable and valid. This study outlines several key steps for verifying the outputs of generative AI.

First, cross-verification with trusted sources or benchmarks is crucial for assessing accuracy and reliability; this study employs a criteria-based approach. Additionally, statistical analysis methods, such as precision, recall, and F1 scores, can be used to evaluate performance, particularly in classification tasks. The results presented in this thesis demonstrate a high F1 score and precision.

Furthermore, consistency checks across different inputs help determine whether the AI produces reliable results. Understanding the model's training data and methodology is also vital for identifying

potential biases and limitations. By implementing these methods, one can ensure that the AI's outputs are both comparable and valid for their intended use.

8.1.1.2 Visualization and Query Interface

This component stores data from the semantic model and integrates it with the National Vulnerability Database (NVD) via an API. Data is stored in the knowledge graph in the form of triples, which can be visualized as nodes and edges.

Knowledge Graph

The knowledge graph facilitates visual representation of the relationships and entities within the IoMT system. The knowledge graph visualization helps stakeholders quickly identify trends, complex patterns, anomalies, and vulnerabilities. Another feature significantly improved with the knowledge graph is the ability to query and evaluate system vulnerabilities effectively. The semantic framework supports advanced query languages, such as SPARQL, which enable complex queries that allow security professionals to extract precise information. For example, queries can be crafted to identify all devices affected by a newly discovered vulnerability, assess the potential impact on patient safety, and recommend appropriate remediation actions.

Evalution of Competency Questions by Querying

The competency questions proposed to develop the semantic model are evaluated through a querying mechanism, where these queries extract insights from the semantic framework to validate the competency questions. This evaluation confirms that the semantic framework is capable of fulfilling the requirements proposed by the study.

8.1.2 Comparative Analysis

The MIoT semantic framework was validated against the existing IoMT-SAF framework. The results of this comparative analysis revealed that the proposed MIoT semantic framework is highly effective in detecting vulnerabilities and anomalies, particularly within remote patient monitoring (RPM) settings. Through automated reasoning, the framework can uncover hidden vulnerabilities, exploits, and attacks, and generate recommendations for mitigation. This finding underscores the framework's applicability and reliability in real-world scenarios, where continuous monitoring and accurate vulnerability detection are crucial.

Overall, the MIoT semantic framework demonstrates its robustness and effectiveness in enhancing the security of the IoMT environment. Its ability to accurately identify vulnerabilities and provide reliable risk assessments makes it a valuable tool for ensuring the safety and integrity of medical systems.

8.2 Findings

8.2.1 Significance of major and supporting findings

This thesis declares six (6) key findings, two (2) of which are posited as major findings of strong significance, and four of which are additional findings that further support the educational and extension value of the overall work.

The finding of greatest significance is the discovery that the addition of automated reasoning (when applied across an ontology and rule set within a semantic model) significantly enhances anomaly detection and subsequent identification of vulnerabilities. Therefore, the application of a semantic model, such as the one described in this thesis, provides a markedly stronger security environment for the Internet of Medical Things (IoMT).

The next most significant finding is the creation of a novel semantic model that offers considerably advanced security positioning for IoMT environments, where there is an essential obligation for healthcare professionals and their systems to protect and secure healthcare data from IoT devices.

There are four supporting findings that are particularly meaningful as they extend the overall security protection for IoMT systems and demonstrate novel approaches that are highly applicable and uniquely relevant to the protection of IoT devices within the healthcare industry:

The first supporting finding is the controlled vocabularies and standards approach, which applies an enriched semantic methodology to the use and application of vocabularies and de-facto standards. Combined with standard language practices, this approach utilizes an ontology-based environment to facilitate the protected interaction of terms, expressions, and language. This is essential for the continuous and unbroken inclusion of critical information.

The second supporting finding is the application of data aggregation and visualization, using an integrated approach with knowledge graphs to maintain real-time storage of known vulnerabilities in medical devices.

The third finding is the combined integration of semantic modelling, data analysis from CVEs, and automated reasoning procedures. This approach provides a more comprehensive outcome in terms of vulnerability detection for remote patient monitoring systems.

The fourth supporting finding is the semantic modelling framework's ability to enhance high-level decision-making through a query mechanism. This mechanism is directly relevant to healthcare professionals, providing early warnings about medical device vulnerabilities related to cyber-attacks.

These findings ae explained in greater detail below the summary – where they follow the order by which they provide direct responses to the thesis Research Questions in the same order that the research questions are asked in the first chapter of this thesis.

8.2.2 Summary of Findings

To address the key research questions in this study, a comprehensive literature review was first conducted to identify research gaps in the domain of IoMT and cybersecurity. The literature review highlighted challenges in healthcare technology, including interoperability, heterogeneity, scalability,

integration, and visualization. In response to these challenges, a semantic framework was developed aimed at optimizing the security posture of the Internet of Medical Things (IoMT) in remote patient monitoring settings. Another significant challenge in healthcare is automation. Existing systems and frameworks often lack the capability to automatically detect anomalies, flaws, or vulnerabilities in medical devices used for data transfer over networks.

The MIoT semantic framework includes a core component, the semantic model, which incorporates the MIoT ontology. By utilizing semantic enrichment, controlled vocabularies, and de-facto standards, the framework ensures seamless communication and data exchange among various systems and medical devices. This interoperability enhances compatibility and integration across different healthcare technologies, creating a cohesive ecosystem for sharing and utilizing health data. However, medical devices, such as BP monitors and heart rate monitors, often come from different vendors with varying specifications and data formats. To address this diversity and heterogeneity, the framework captures semantic information from medical devices manufactured by different vendors.

Additionally, the semantic framework facilitates the integration of various data sources, including the MIoT ontology and NVD data (CVE and CVSS information), by providing a common semantic model. The knowledge graph in the semantic framework serves as a linked-node database, representing knowledge in a graph format. Entities and relationships from the semantic model are represented in a flexible and efficient manner, facilitating integration, visualization, and querying processes. The efficiency of data integration processes is crucial, as poorly integrated data may result in slower query execution due to additional processing overhead. The results of running SPARQL queries indicate that the proposed MIoT semantic model is efficiently integrated with the MIoT knowledge graph.

Furthermore, the framework's scalability in terms of data volume is evident. Initial experiments conducted with limited data from the NVD database show that it can easily handle live data streams acquired through the NVD API, demonstrating its ability to accommodate larger datasets.

The most important aspect of the MIoT Semantic framework is automated reasoning. The semantic model contains logical rules and algorithms used to infer new knowledge or insights from existing knowledge by analyzing data and detecting patterns in the ruleset. In this study, attacks, and other anomalies due to vulnerabilities are modeled and analyzed. This study demonstrates that the proposed semantic model is capable of detecting vulnerabilities from integrated data from CVEs by performing reasoning. It infers new facts that indicate possible attacks exploited due to certain vulnerabilities, adverse side effects, and suggests mitigations and recommendations to enhance system security.

In summary, the proposed semantic framework optimizes medical data in IoMT infrastructure to support security posture by utilizing semantic web technologies. The framework addresses key issues related to modeling and visualization by introducing a novel semantic model and representing data in a meaningful way, thus supporting interoperability, heterogeneity, scalability, and integration of data. Furthermore, the reasoning approach detects the vulnerabilities automaticaly, and suggests their consequences along with mitigation recommendations to secure the system.

In the following sections, further details about findings are provided in key points in the light of the research questions (discussed in Section 1.3).

8.2.3 Key Findings

- **Research Question 1 (RQ1):** How can data be optimized to support the cybersecurity posture of Remote Patient Monitoring Systems on the Internet of Medical Things (IoMT)?

  To address RQ1, the study investigated the optimization of data to support the cybersecurity posture of IoMT-based remote patient monitoring systems. The findings revealed several key strategies:

  (a) **Semantic Modeling:** The semantic framework enhances the security posture of IoMT by effectively utilizing semantic web technologies. The study shows that ontology modeling effectively represents healthcare data by providing its semantics and annotations for representing healthcare data in IoMT systems. This approach facilitates meaningful data aggregation, addressing challenges related to interoperability, heterogeneity, and integration.

  By employing semantic web technologies, the framework can capture and utilize the rich context and relationships inherent in healthcare data, making it easier to draw meaningful insights and connections. Ontology modeling ensures that data from diverse sources can be harmonized and understood in a unified manner, thereby improving data quality and consistency. This is particularly important in IoMT systems, where data originates from a wide array of medical devices and information systems, each with its own data formats and standards.

  (b) **Automated Reasoning:** The semantic model's automated reasoning capabilities enable the detection of new knowledge or insights from existing data, identifying vulnerabilities and suggesting mitigations.The framework uses a ruleset based on logic, making the system more robust and efficient. The reasoning capabilities of the framework enable the identification of potential vulnerabilities and anomalies in IoMT systems based on these logics. The reasoning results show that vulnerabilities and anomalies can be detected automatically without looking at the vulnerability database, thereby strengthening security measures in remote monitoring settings.

  (c) **Controlled Vocabularies and Standards:** Utilizing semantic enrichment, controlled vocabularies, and de-facto standards such as RDF ensures seamless communication and data exchange among various systems and medical devices. This approach allows for consistent terminology and understanding across different platforms, reducing the likelihood of misinterpretation and errors. The use of controlled vocabularies aids in maintaining a standardized language, which is essential for the accurate identification and classification of vulnerabilities.

  Furthermore, adhering to established standards like RDF (Resource Description Framework) facilitates interoperability between disparate systems, enabling them to share and interpret data efficiently. This interoperability is crucial in a diverse ecosystem like MIoT, where multiple devices and systems must work together seamlessly. By incorporating these

standards, the framework not only enhances data integration and retrieval but also ensures that the information is accessible and usable across various applications and stakeholders.

(d) **Data Aggregation and visualization:** The efficient integration of data within the MIoT semantic model ensures that poorly integrated data, which could result in slower query execution, is avoided. The MIoT knowledge graph integrated into the framework efficiently acquires data from the National Vulnerability Database (NVD), ensuring a comprehensive and up-to-date repository of known vulnerabilities in medical devices. Automatic retrieval of data from the NVD enables the framework to stay abreast of the latest security threats and vulnerabilities, facilitating timely identification and mitigation of risks in IoMT systems.

Additionally, data visualization plays a crucial role in understanding and analyzing the aggregated data. Visual tools, such as interactive dashboards and graph-based representations, help in identifying patterns and trends within the data. These visualizations enable stakeholders to quickly grasp complex information, making it easier to pinpoint critical vulnerabilities and take necessary actions. By employing advanced visualization techniques, the framework enhances the user's ability to monitor and manage security risks effectively, ensuring that decision-makers have access to clear and actionable insights.

- **Research Question 2 (RQ2):** How can vulnerabilities be detected automatically within remote patient monitoring systems?

  (a) **Vulnerability Detection by Automated Reasoning:** The framework uses a ruleset based on logic, making the system more robust and efficient. Its reasoning capabilities enable the identification of potential vulnerabilities and anomalies in IoMT systems. The results demonstrate that vulnerabilities and anomalies can be detected automatically, even without referring to the vulnerability database, thereby enhancing security measures in remote monitoring settings. Key points include:

  - **Vulnerability Detection:** The semantic model incorporates logical rules and algorithms for analyzing data, detecting patterns, and identifying vulnerabilities, exploits, and attacks.
  - **Integrated Data Analysis:** By integrating data from CVEs and performing reasoning, the model can infer new facts that indicate possible attacks due to certain vulnerabilities and suggest mitigations to enhance system security.
  - **Automated Reasoning:** Automated reasoning processes analyze data and detect patterns within the ruleset, inferring new knowledge about potential vulnerabilities, attacks, and their consequences. This capability to automatically detect anomalies, flaws, or vulnerabilities in medical devices used for data transfer over networks addresses a significant challenge in healthcare automation.

  (b) **Improved Querying and Decision-Making:** The framework supports an efficient querying mechanism, enabling healthcare providers to extract valuable insights from IoMT data. For example, complex queries can notify doctors and healthcare providers about new vulnerabilities in the system or whether any medical device is vulnerable. It also assesses

the impact of vulnerabilities on cybersecurity requirements such as Confidentiality, Integrity, and Availability (CIA), allowing for easy countermeasures based on severity levels. This feature encourages timely decision-making processes, enhancing the overall efficiency and effectiveness of IoMT systems.

The proposed semantic framework optimizes medical data in IoMT infrastructure to support security posture by utilizing semantic web technologies. It addresses key issues related to modeling and visualization by introducing a novel semantic model that supports interoperability, heterogeneity, scalability, and data integration. The reasoning approach within the framework detects vulnerabilities automatically and suggests mitigations to secure the system, thereby enhancing the cybersecurity posture of remote patient monitoring systems in the IoMT environment.

8.3 Limitation and Challenges of Study

(a) Limited Information on Medical Device Specifications

The literature and available online resources often lack explicit details about the firmware, version, operating system, or software utilized in the manufacturing of medical devices. Vendors and manufacturers typically provide product specifications related to weight, dimensions, functions, and connectivity. However, they seldom disclose the standards, compliance protocols, software versions, or operating systems used in their products.

This lack of detailed information poses significant challenges in modeling and identifying potentially vulnerable components. Without this information, it is difficult to anticipate which parts of the device might be susceptible to security threats and therefore require preemptive mitigation measures. Addressing these gaps is crucial for enhancing the security and reliability of medical devices in the IoMT ecosystem.

(b) Lack of Publicly Availabe Dataset

Most publicly available datasets, such as MIMIC III [251; 252] and SnomedCT [195; 200] are laboratory datasets that provide clinical or electronic health record (EHR) readings. To the best of my knowledge, there are no publicly available datasets specifically designed for detecting vulnerabilities or cyberattacks in remote patient monitoring systems. This gap in publicly available data poses a significant challenge for researchers and practitioners aiming to enhance the cybersecurity of IoMT environments.

(c) Privacy and Ethical Issues

Due to the scope of this study, the research focuses solely on the security aspects of the Internet of Medical Things (IoMT) and does not address the privacy or ethical issues. However, it is important to acknowledge that these areas are critical and present significant challenges.

Privacy concerns in IoMT revolve around the sensitive nature of medical data, which requires stringent measures to protect patient information from unauthorized access and breaches. Ethical

issues include ensuring patient consent, data ownership, and the responsible use of health data. These aspects are complex and require comprehensive frameworks and policies to address effectively.

While this study provides a robust approach to enhancing the security of IoMT systems, future research should aim to integrate privacy and ethical considerations to develop a holistic solution that not only protects against vulnerabilities and attacks but also safeguards patient rights and data integrity. Addressing these challenges is essential for the widespread adoption and trust in IoMT technologies.

8.4 Summary of the chapter

This chapter discusses the experimental results and findings of the comprehensive semantic framework for the Internet of Medical Things (IoMT). The results demonstrate the high effectiveness of the proposed framework in detecting vulnerabilities and anomalies, particularly in remote patient monitoring systems. Key findings highlight the framework's robust data modeling, efficient data integration, and enhanced querying capabilities, which collectively improve the security posture of IoMT environments. Additionally, this chapter also discusses the Limitations and Challenges. However, the study primarily focuses on security aspects, leaving privacy and ethical issues unaddressed. Future research should integrate these critical areas to develop a holistic approach for IoMT security.

Chapter 9

Conclusion and Future work

This chapter presents the conclusion of the thesis and outlines potential directions for future research.

9.1 Conclusion of the Thesis

The significance of the Internet of Medical Things (IoMT), particularly in remote patient monitoring, cannot be overstated. IoMT technologies have revolutionized healthcare by enabling continuous monitoring and real-time data transmission, significantly improving patient outcomes and reducing healthcare costs. However, the integration of IoMT devices into healthcare systems introduces numerous security challenges. Vulnerability detection in these settings is crucial, as any security breach can lead to severe consequences, including unauthorized access to sensitive patient data, disruption of medical services, and potential harm to patients. Therefore, robust and efficient vulnerability detection mechanisms are essential to ensure the security and reliability of IoMT environments.

This thesis presents a comprehensive study on enhancing the cybersecurity posture of the Internet of Medical Things (IoMT) through the development and implementation of a semantic framework. The framework, composed of a semantic model and a knowledge graph, successfully integrates medical device data with information from the National Vulnerability Database (NVD). By employing the MIoT ontology and leveraging automated reasoning, the framework demonstrates a high effectiveness in detecting vulnerabilities and anomalies within remote patient monitoring systems. The rigorous evaluation, utilizing standardized knowledge engineering methodologies and generative AI models, validates the robustness and applicability of the proposed solution in real-world settings.

Key findings from the study underscore the framework's capabilities in robust data modeling, efficient data integration, and enhanced querying, all of which contribute significantly to improving the security of IoMT environments. Despite the success, the study acknowledges its limitations, particularly the focus on security aspects while leaving privacy and ethical issues unaddressed. Addressing these areas is critical for the holistic development of IoMT security. Future research should aim to integrate privacy and ethical considerations, ensuring that the framework not only protects against cyber threats but also safeguards patient data integrity and upholds ethical standards in healthcare technology. Furthermore, this framework can be extended to integrate the MITRE ATT&CK framework and use the NLP techniques for syntactic analysis.

9.2 Future Work

(a) In this study, the researcher focuses on the semantics of medical devices and their related entities. However, by analyzing syntax, the information about vulnerabilities can be enhanced. One of the techniques used for syntax modelling is NLP (Natural Language Processing). This MIoT semantic Framework can be improved by performing syntactic analysis of medical devices in future by using NLP techniques.

(b) Another avenue for future research is leveraging the full extension of the MITRE ATT&CK framework to map the relationships between common attack techniques used by adversaries and widely accepted standards such as ISO 27001 and NIST SP 800-53. By utilizing the MIoT semantic framework and by updating a few entities in MIoT ontology, organizations can enhance their ability to identify and mitigate potential attack vectors targeting their assets and business operations. This approach is also relatively straightforward and does not require extensive effort or research, as MITRE has already established mappings to NIST SP 800-53 controls, which can be seamlessly integrated into existing or new ontologies.

(c) Addressing privacy and ethical issues in IoT health systems is crucial for maintaining patient trust, ensuring compliance with legal requirements, and promoting the ethical use of health data. By implementing strong data protection measures, ensuring transparency and accountability, and respecting patient rights, IoT health systems can effectively safeguard patient privacy and uphold ethical standards. The MIoT ontology can be extended with new entities that specifically address privacy and ethical concerns, thereby enhancing the security and integrity of IoMT environments. This extension will ensure that the framework not only detects vulnerabilities but also protects patient data and adheres to ethical guidelines.

The findings of this work demonstrate the challenge in terms of striking a balance between important data sharing on Medical IoT devices and enabling that data sharing to continue along with the satisfaction of the various privacy concerns with regard to medical data. Medical IoT devices operate across borders and in different regions across the globe. The differences between regions such as Europe (with the GDPR) and Asia, (which holds and different set of privacy values), remains a contested issue. Even Australia which is an observer but not a signatory to the GDPR, shares medical data from IoTs in such a way that a commitment to shared data in one country, can reveal a breach of privacy in another country.

These challenges are not easily overcome, but nevertheless they must remain alongside the increased vigilance of IoT security. As new security concerns evolve, privacy concerns retain and expand their multi-faceted regulatory boundaries. Just like cyber criminals, medical IoT devices do not recognise nation state borders. They operate continuously and require ongoing watchful observation. Globally, privacy and security continue to operate hand in hand.

Bibliography

[1] "13 biggest data breaches in australia [updated 2024]." https://www.upguard.com/blog/biggest-data-breaches-australia, 2024.

[2] "Data breach: Broward health warns 1.3 million patients, staff of 'medical identity theft'." https://www.zdnet.com/article/broward-health-warns-1-3-million-patients-staff-of-medical-\identity-theft-after-data-breach/, 2024.

[3] "Broward health data breach impacts 1.3 million people - securityweek." Accessed [Online]: Nov. 07, 2023. . Available:https://www.securityweek.com/broward-health-data-breach-impacts-13-million-people/, 2024.

[4] OAIC, "Notifiable data breaches report: January to june 2023," tech. rep., 2023. Accessed: July. 07, 2023. [Online]. Available: https://www.oaic.gov.au/__data/assets/pdf_file/0020/83702/OAIC-Notifiable-data-breaches-report-January-to-June-2023-final.pdf.

[5] "Knowledge organization systems: An overview," 2024. Available [Online]: https://www.clir.org/pubs/reports/pub107/.

[6] G. M. Hodge and D. L. Federation, Systems of knowledge organization for digital libraries: beyond traditional authority files. Digital Library Federation, Council on Library and Information Resources, 2000.

[7] T. Baker, S. Bechhofer, A. Isaac, A. Miles, G. Schreiber, and E. Summers, "Key choices in the design of simple knowledge organization system (skos)," Journal of Web Semantics, vol. 20, pp. 35–49, 2013. https://doi.org/10.1016/j.websem.2013.05.001.

[8] A. Luschi, C. Petraccone, G. Fico, L. Pecchia, and E. Iadanza, "Semantic ontologies for complex healthcare structures: A scoping review," IEEE Access, vol. 11, pp. 19228–19246, 2023. https://doi.org/10.1109/ACCESS.2023.3248969.

[9] D. Dai and S. Boroomand, "A review of artificial intelligence to enhance the security of big data systems: State-of-art, methodologies, applications, and challenges," Archives of Computational Methods in Engineering, vol. 29, no. 2, pp. 1291–1309, 2022. https://doi.org/10.1007/s11831-021-09628-0.

[10] Z. Zhang et al., "Developing an ontology for representing the domain knowledge specific to non-pharmacological treatment for agitation in dementia," Alzheimer's and Dementia: Translational Research and Clinical Interventions, vol. 6, no. 1, pp. 1–17, 2020. https://doi.org/10.1002/trc2.12061.

[11] G. Sripriyanka and A. Mahendran, A study on security privacy issues and solutions in internet of medical things-A review. Elsevier Inc., 2020. https://doi.org/10.1016/B978-0-12-821187-8.00006-X.

[12] C. M. Keet, An Introduction to Ontology Engineering. Springer, 2018. https://people.cs.uct.ac.za/~mkeet/files/OEbook.pdf.

[13] K. S. Bughio, D. M. Cook, and S. A. A. Shah, "Developing a novel ontology for cybersecurity in internet of medical things-enabled remote patient monitoring," Sensors, vol. 24, Apr. 2024. https://doi.org/10.3390/s24092804.

[14] "Regulation of medical devices in the european union," European Journal of Health Law, 2021. https://health.ec.europa.eu/medical-devices-sector/new-regulations_en.

[15] O. A. Shorman, B. A. Shorman, M. Al-Khassaweneh, and F. Alkahtani, "A review of internet of medical things (iomt) - based remote health monitoring through wearable sensors: A case study for diabetic patients," Indonesian Journal of Electrical Engineering and Computer Science, vol. 20, pp. 414–422, Oct. 2020. https://doi.org/10.11591/ijeecs.v20.i1.pp414-422.

[16] "Web standards w3c," 2023. Available [ONLINE]: https://www.w3.org/standards/semanticweb/., Accessed: Dec. 10, 2023.

[17] "Resource description framework (rdf): Concepts and abstract syntax," w3c recommendation, W3C, 2014. https://www.w3.org/TR/rdf-concepts/.

[18] "Xml schema part 1: Structures second edition," w3c recommendation, W3C, 2004. https://www.w3.org/TR/xmlschema-1/.

[19] "Framework for improving critical infrastructure cybersecurity," tech. rep., National Institute of Standards and Technology, 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[20] "Hl7 fhir," 2024. Available [ONLINE]:https://www.hl7.org/fhir/. Accessed on: Jan. 10, 2024.

[21] "U.s. department of health and human services," 2024. [Online]. Available: https://www.hhs.gov/hipaa/index.html.Accessed [ONLINE]: Jan. 12, 2024.

[22] K. S. Bughio, D. M. Cook, and S. A. A. Shah, "Challenges and solutions in securing medical iot systems," International Journal of Information Security, 2024.

[23] R. Mansell, "Information and communication technology policy research in the united kingdom: A perspective," Canadian Journal of Communication, vol. 19, no. 1, pp. 1–11, 1994. https://doi.org/10.22230/cjc.1994v19n1a792.

[24] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey," Computer Networks, vol. 38, pp. 393–422, 2002. https://doi.org/10.1109/WAINA.2009.192.

[25] M. B. M. Kamel and L. E. George, "Remote patient tracking and monitoring system," International Journal of Computer Science and Mobile Computing, vol. 2, pp. 88–94, 2013.

[26] M. Bennasar et al., "Knowledge-based architecture for recognising activities of older people," in 23rd International Conference on Knowledge-Based and Intelligent Information & Engineering Systems, vol. 159, pp. 590–599, 2019. https://doi.org/10.1016/j.procs.2019.09.214.

[27] B. Hammi, S. Zeadally, R. Khatoun, and J. Nebhen, "Survey on smart homes: Vulnerabilities, risks, and countermeasures," Comput Secur, vol. 117, no. March, 2022. https://doi.org/10.1016/j.cose.2022.102677.

[28] A. Kumar and K. Chatterjee, "Securing internet of medical devices using energy efficient blockchain for healthcare 4.0," Cluster Comput, 2024. https://doi.org/10.1007/s10586-024-04437-z.

[29] R. Al-Shaqi, M. Mourshed, and Y. Rezgui, "Progress in ambient assisted systems for independent living by the elderly," Springerplus, vol. 5, no. 1, 2016. https://doi.org/10.1186/s40064-016-2272-8.

[30] L. A. Despins et al., "Using sensor signals in the early detection of heart failure: A case study," J Gerontol Nurs, vol. 46, no. 7, pp. 41–46, 2020. https://doi.org/10.3928/00989134-20200605-07.

[31] S. Alromaihi, W. Elmedany, and C. Balakrishna, "Cyber security challenges of deploying iot in smart cities for healthcare applications," in Proceedings - 2018 IEEE 6th International Conference on Future Internet of Things and Cloud Workshops, W-FiCloud 2018, pp. 140–145, 2018. https://doi.org/10.1109/W-FiCloud.2018.00028.

[32] A. Mavrogiorgou, A. Kiourtis, and D. Kyriazis, "Identification of iot medical devices apis through ontology mapping techniques," in EAI/Springer Innovations in Communication and Computing, pp. 39–54, 2020. https://doi.org/10.1007/978-3-030-30335-8_4.

[33] W. E. Zhang et al., "The 10 research topics in the internet of things," in Proceedings - 2020 IEEE 6th International Conference on Collaboration and Internet Computing, CIC 2020, pp. 34–43, 2020. https://doi.org/10.1109/CIC50333.2020.00015.

[34] Pritika, B. Shanmugam, and S. Azam, "Risk assessment of heterogeneous iomt devices: A review," Technologies (Basel), vol. 11, no. 1, 2023. https://doi.org/10.3390/technologies11010031.

[35] M. Wazid and P. Gope, "Backm-eha: A novel blockchain-enabled security solution for iomt-based e-healthcare applications," ACM Trans Internet Technol, vol. 23, no. 3, 2023. https://doi.org/10.1145/3511898.

[36] M. M. Dhanvijay and S. C. Patil, "Internet of things: A survey of enabling technologies in healthcare and its applications," Computer Networks, vol. 153, pp. 113–131, 2019. https://doi.org/10.1016/j.comnet.2019.03.006.

[37] M. Wazid, A. K. Das, J. J. P. C. Rodrigues, S. Shetty, and Y. Park, "Iomt malware detection approaches: Analysis and research challenges," IEEE Access, vol. 7, pp. 182459–182476, 2019. https://doi.org/10.1109/ACCESS.2019.2960412.

[38] L. L. Mitchell et al., "'it's like a cyber-security blanket': The utility of remote activity monitoring in family dementia care," Journal of Applied Gerontology, vol. 39, no. 1, pp. 86–98, 2020. https://doi.org/10.1177/0733464818760238.

[39] K. S. Bughio and L. F. Sikos, Knowledge Organization Systems to Support Cyber-Resilience in Medical Smart Home Environments. Springer International Publishing, 2023. https://doi.org/10.1007/978-3-031-24946-4_5.

[40] G. I. Rajathi, R. J. Elton, M. B. Mol, L. Prinza, G. J. Prasath, and J. M. Rajarathnam, Transfiguration of Health Care from Human to Machine Touchpoint—A Prospect or a Pittance? Elsevier Inc., 2023. https://doi.org/10.1016/B978-0-323-89872-0.00010-1.

[41] A. Meola, "Iot in healthcare 2021: Companies, medical devices, and use cases," 2021. [Online]. Available:https://www.businessinsider.com/iot-healthcare.

[42] "Government probing 'data breach' of 8 crore indians from icmr covid site - times of india," 2024. Available [ONLINE] https://timesofindia.indiatimes.com/india/government-probing-data-breach-of-8-crore-indians-from-icmr-\covid-site/articleshow/104835828.cms , Accessed on: 10 Jan 2024.

[43] T. G. Administration, "Medical device cyber security guidance for industry," tech. rep., 2021. Available [Online]: https://www.tga.gov.au/sites/default/files/medical-device-cyber-security-guidance-industry.pdf.

[44] P. Doyle, "Healthcare breaches on the rise in 2022." [Online]. Available https://www.techtarget.com/searchsecurity/news/252521771/Healthcare-breaches-on-the-rise.

[45] D. Bonderud, "Top healthcare data breach statistics of 2023," 2023. Persona.

[46] H. Journal, "More than 4 million individuals affected by cyberattack on independent living systems," 2023. THE HIPAA JOURNAL.

[47] "Asd cyber threat report 2022-2023," 2023. Accessed: Dec. 09, 2023. [Online]. Available: https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023.

[48] K. S. Bughio, D. M. Cook, and S. A. A. Shah, "Investigating the intersections of vulnerability detection and iomts in healthcare, a scoping review protocol for remote patient monitoring," Research, Society and Development, vol. 13, no. 6, 2024. https://rsdjournal.org/index.php/rsd/article/view/46080.

[49] S. Banyal, D. Mehra, Amartya, S. Banyal, D. K. Sharma, and U. Ghosh, Computational Intelligence in Healthcare with Special Emphasis on Bioinformatics and Internet of Medical Things, pp. 145–170. 2022. https://doi.org/10.1007/978-3-030-81473-1_7.

[50] S. Razdan and S. Sharma, "Internet of medical things (iomt): Overview, emerging technologies, and case studies," IETE Technical Review (Institution of Electronics and Telecommunication Engineers, India), vol. 39, no. 4, pp. 775–788, 2022.

[51] Statista, "Prognosis of worldwide spending on the internet of things (iot) from 2018 to 2023," 2023. [Online]. Available:https://www.statista.com/statistics/668996/worldwide-expenditures-for-the-internet-of-things/.

[52] J. Srivastava, S. Routray, S. Ahmad, and M. M. Waris, "Internet of medical things (iomt)-based smart healthcare system: Trends and progress," Comput Intell Neurosci, vol. 2022, 2022. https://doi.org/10.1155/2022/7218113.

[53] Y. Sun, F. P. W. Lo, and B. Lo, "Security and privacy for the internet of medical things enabled healthcare systems: A survey," IEEE Access, vol. 7, pp. 183339–183355, 2019. https://doi.org/10.1109/ACCESS.2019.2960617.

[54] A. Algarni, "A survey and classification of security and privacy research in smart healthcare systems," IEEE Access, vol. 7, pp. 101879–101894, 2019. https://doi.org/10.1109/ACCESS.2019.2930962.

[55] A. H. M. Aman, W. H. Hassan, S. Sameen, Z. S. Attarbashi, M. Alizadeh, and L. A. Latiff, "Iomt amid covid-19 pandemic: Application, architecture, technology, and security," Journal of Network and Computer Applications, vol. 174, Jan. 2021. https://doi.org/10.1016/j.jnca.2020.102886.

[56] A. E. Khaled, "Internet of medical things (iomt): Overview, taxonomies, and classifications," Journal of Computer and Communications, vol. 10, no. 08, pp. 64–89, 2022. https://doi.org/10.4236/jcc.2022.108005.

[57] T. P. Latchoumi, R. Swathi, P. Vidyasri, and K. Balamurugan, "Develop new algorithm to improve safety on wmsn in health disease monitoring," in 2022 International Mobile and Embedded Technology Conference, MECON 2022, pp. 357–362, Institute of Electrical and Electronics Engineers Inc., 2022. https://doi.org/10.1109/MECON53876.2022.9752178.

[58] S. B. Weber, S. Stein, M. Pilgermann, and T. Schrader, "Attack detection for medical cyber-physical systems-a systematic literature review," IEEE Access, vol. 11, no. May, pp. 41796–41815, 2023. https://doi.org/10.1109/ACCESS.2023.3270225.

[59] S. Majumder et al., "Smart homes for elderly healthcare—recent advances and research challenges," Sensors (Switzerland), vol. 17, no. 11, 2017. https://doi.org/10.3390/s17112496.

[60] S. J. Bhasha and P. Sunita, "An iot-based body area network in medical care system: Related challenges and issues," International Journal of Innovative Technology and Exploring Engineering, vol. 9, no. 1, pp. 541–546, 2019. https://doi.org/10.35940/ijitee.L2545.119119.

[61] K. Lopatina, V. A. Dokuchaev, and V. V. Maklachkova, "Data risks identification in healthcare sensor networks," in 2021 International Conference on Engineering Management of Communication and Technology, EMCTECH 2021 - Proceedings, pp. 1–7, 2021. https://doi.org/10.1109/EMCTECH53459.2021.9619178.

[62] F. A. C. D. D. Farias, C. M. Dagostini, Y. D. A. Bicca, V. F. Falavigna, and A. Falavigna, "Remote patient monitoring: A systematic review," Telemedicine and e-Health, vol. 26, no. 5, pp. 576–583, 2020. https://doi.org/10.1089/tmj.2019.0066.

[63] N. Sharma et al., "A smart ontology-based iot framework for remote patient monitoring," Biomed Signal Process Control, vol. 68, Jul. 2021. https://doi.org/10.1016/j.bspc.2021.102717.

[64] G. L. Tortorella, F. S. Fogliatto, A. M. C. Vergara, R. Vassolo, and R. Sawhney, "Healthcare 4.0: trends, challenges and research directions," Production Planning and Control, vol. 31, pp. 1245–1260, Nov. 2020. https://doi.org/10.1080/09537287.2019.1702226.

[65] L. P. Malasinghe, N. Ramzan, and K. Dahal, "Remote patient monitoring: a comprehensive study," J Ambient Intell Humaniz Comput, vol. 10, no. 1, pp. 57–76, 2019. https://doi.org/10.1007/s12652-017-0598-x.

[66] A. Dridi, S. Sassi, and S. Faiz, "Towards a semantic medical internet of things," in Proceedings of IEEE/ACS International Conference on Computer Systems and Applications, AICCSA, vol. 2017-Octob, pp. 1421–1428, 2018. https://doi.org/10.1109/AICCSA.2017.194.

[67] Y. He, A. Aliyu, M. Evans, and C. Luo, "Health care cybersecurity challenges and solutions under the climate of covid-19: Scoping review," J Med Internet Res, vol. 23, no. 4, 2021. https://doi.org/10.2196/21747.

[68] W. Priestman, T. Anstis, I. G. Sebire, S. Sridharan, and N. J. Sebire, "Phishing in healthcare organisations: threats, mitigation and approaches," pp. 1–6, 2019. https://doi.org/10.1136/bmjhci-2019-100031.

[69] J. Dofe, A. Nguyen, and A. Nguyen, "Unified countermeasures against physical attacks in internet of things - a survey," in Proceedings - 2021 IEEE International Symposium on Smart Electronic Systems, iSES 2021, pp. 194–199, Institute of Electrical and Electronics Engineers Inc., 2021. https://doi.org/10.1109/iSES52644.2021.00053.

[70] M. Zhang, A. Raghunathan, and N. K. Jha, "Medmon: Securing medical devices through wireless monitoring and anomaly detection," IEEE Trans Biomed Circuits Syst, vol. 7, no. 6, pp. 871–881, 2013. https://doi.org/10.1109/TBCAS.2013.2245664.

[71] F. Alsubaei, A. Abuhussein, and S. Shiva, "Security and privacy in the internet of medical things: Taxonomy and risk assessment," in Proceedings - 2017 IEEE 42nd Conference on Local Computer Networks Workshops, LCN Workshops 2017, no. September 2018, pp. 112–120, 2017. https://doi.org/10.1109/LCN.Workshops.2017.72.

[72] M. Ibrahim, A. Alsheikh, and A. Matar, "Attack graph modeling for implantable pacemaker," Biosensors (Basel), vol. 10, no. 2, pp. 1–12, 2020. https://doi.org/10.3390/bios10020014.

[73] V. Hassija, V. Chamola, B. C. Bajpai, Naren, and S. Zeadally, "Security issues in implantable medical devices: Fact or fiction?," Sustain Cities Soc, vol. 66, no. April 2020, 2021. https://doi.org/10.1016/j.scs.2020.102552.

[74] N. Roy, A. Misra, D. Cook, and D. Cook, "Ambient and smartphone sensor assisted adl recognition in multi-inhabitant smart environments," J Ambient Intell Humaniz Comput, vol. 7, no. 1, pp. 1–19, 2016. https://doi.org/10.1007/s12652-015-0294-7.

[75] S. Hamid, N. Z. Bawany, A. H. Sodhro, A. Lakhan, and S. Ahmed, "A systematic review and iomt based big data framework for covid-19 prevention and detection," Electronics (Switzerland), vol. 11, no. 17, 2022. https://doi.org/10.3390/electronics11172777.

[76] L. Lu et al., "Wearable health devices in health care: Narrative systematic review."

[77] X. Li, B. Tao, H. N. Dai, M. Imran, D. Wan, and D. Li, "Is blockchain for internet of medical things a panacea for covid-19 pandemic?," Pervasive Mob Comput, vol. 75, Aug. 2021. https://doi.org/10.1016/j.pmcj.2021.101434.

[78] S. Swayamsiddha and C. Mohanty, "Application of cognitive internet of medical things for covid-19 pandemic," Diabetes and Metabolic Syndrome: Clinical Research and Reviews, vol. 14, pp. 911–915, Sep. 2020. https://doi.org/10.1016/j.dsx.2020.06.014.

[79] S. Dash, S. K. Shakyawar, M. Sharma, and S. Kaushik, "Big data in healthcare: management, analysis and future prospects," J Big Data, vol. 6, Dec. 2019. https://doi.org/10.1186/s40537-019-0217-0.

[80] A. Pazienza, G. Polimeno, F. Vitulano, and Y. Maruccia, "Towards a digital future: An innovative semantic iot integrated platform for industry 4.0, healthcare, and territorial control," in Conf Proc IEEE Int Conf Syst Man Cybern, vol. 2019-Octob, pp. 587–592, 2019. https://doi.org/10.1109/SMC.2019.8914662.

[81] F. Cicirelli, G. Fortino, A. Giordano, A. Guerrieri, G. Spezzano, and A. Vinci, "On the design of smart homes: A framework for activity recognition in home environment," J Med Syst, vol. 40, no. 9, 2016. https://doi.org/10.1007/s10916-016-0549-7.

[82] B. Moazzami, N. Razavi-Khorasani, A. D. Moghadam, E. Farokhi, and N. Rezaei, "Covid-19 and telemedicine: Immediate action required for maintaining healthcare providers well-being," Journal of Clinical Virology, vol. 126, May 2020. https://doi.org/10.1016/j.jcv.2020.104345.

[83] M. K. Hasan et al., "A review on security threats, vulnerabilities, and counter measures of 5g enabled internet-of-medical-things," IET Communications, vol. 16, no. 5, pp. 421–432, 2022. https://doi.org/10.1049/cmu2.12301.

[84] W. G. J. Halfond, J. Viegas, and A. Orso, "A classification of sql injection attacks and countermeasures," 2006.

[85] Q. Kerns, B. Payne, and T. Abegaz, "Double-extortion ransomware: A technical analysis of maze ransomware," in Lecture Notes in Networks and Systems, pp. 82–94, Springer Science and Business Media Deutschland GmbH, 2022. https://doi.org/10.1007/978-3-030-89912-7_7.

[86] A. C. S. Centre, "2020-013 ransomware targeting australian aged care and healthcare sectors," tech. rep., 2022. pp. 1–6.

[87] T. Mahler, Y. Elovici, and Y. Shahar, "A new methodology for information security risk assessment for medical devices and its evaluation," 2020.

[88] K. L. Lueth, "Iot 2022 in review: The 10 most relevant iot developments of the year." Accessed: Nov. 22, 2023. [Online]. https://iot-analytics.com/iot-2020-in-review/.

[89] A. A. Khan, A. A. Wagan, A. A. Laghari, A. R. Gilal, I. A. Aziz, and B. A. Talpur, "Biomt: A state-of-the-art consortium serverless network architecture for healthcare system using blockchain smart contracts," IEEE Access, vol. 10, pp. 78887–78898, 2022. https://doi.org/10.1109/ACCESS.2022.3194195.

[90] A. Alsuwaidi, A. Hassan, F. Alkhatri, H. Ali, M. Qbeaah, and S. Alrabaee, "Security vulnerabilities detected in medical devices," in Proceedings - 2020 12th Annual Undergraduate Research Conference on Applied Computing, URC 2020, 2020. https://doi.org/10.1109/URC49805.2020.9099192.

[91] L. A. Times, "Hollywood hospital pays $17,000 in bitcoin to hackers; fbi investigating."

[92] D. R. Farringer, "Send us the bitcoin or patients will die: Addressing the risks of ransomware attacks on hospitals," Seattle Univ Law Rev, vol. 40, no. 3, pp. 16–23, 2017.

[93] T. Mahler et al., "Know your enemy: Characteristics of cyber-attacks on medical imaging devices," 2018. [Online]. Availablehttp://arxiv.org/abs/1801.05583.

[94] G. S. Gaba, M. Hedabou, P. Kumar, A. Braeken, M. Liyanage, and M. Alazab, "Zero knowledge proofs based authenticated key agreement protocol for sustainable healthcare," Sustain Cities Soc, vol. 80, no. January, 2022. https://doi.org/10.1016/j.scs.2022.103766.

[95] L. Irwin, "Indiana hospital pays $55,000 after ransomware attack." IT Governance USA Blog, p. Accessed online on 30th Nov 2023.

[96] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Bedgehealth: A decentralized architecture for edge-based iomt networks using blockchain," IEEE Internet Things J, vol. 8, no. 14, pp. 11743–11757, 2021. https://doi.org/10.1109/JIOT.2021.3058953.

[97] S. Cheu, "Cyber attack warning: Providers advised to take precautions," p. 8, 2020.

[98] G. Okeyo, L. Chen, and H. Wang, "Combining ontological and temporal formalisms for composite activity modelling and recognition in smart homes," Future Generation Computer Systems, vol. 39, pp. 29–43, 2014. https://doi.org/10.1016/j.future.2014.02.014.

[99] L. Coventry and D. Branley, "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward," Maturitas, vol. 113, pp. 48–52, 2018. https://doi.org/10.1016/j.maturitas.2018.04.008.

[100] B. B. Frey, Health Insurance Portability and Accountability Act, vol. 1996, pp. 12–14. 2018. https://doi.org/10.4135/9781506326139.n302.

[101] S. Nasiri, F. Sadoughi, M. H. Tadayon, and A. Dehnad, "Security requirements of internet of things-based healthcare system: A survey study," Acta Informatica Medica, vol. 27, no. 4, pp. 253–258, 2019. https://doi.org/10.5455/aim.2019.27.253-258.

[102] T. Yaqoob, H. Abbas, and M. Atiquzzaman, "Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices-a review," IEEE Communications Surveys and Tutorials, vol. 21, no. 4, pp. 3723–3768, 2019. https://doi.org/10.1109/COMST.2019.2914094.

[103] "Semantic web." WIKIPEDIA The Free Encyclopedia. [Online]. Available: note = http://ci.nii.ac.jp/naid/40005540465/.AccessedOn[07-02-2024].

[104] S. Kakad and S. Dhage, "Knowledge graph and semantic web model for cross domain," J Theor Appl Inf Technol, vol. 100, no. 16, pp. 5202–5218, 2022.

[105] J. Ye et al., "Semantic web technologies in pervasive computing: A survey and research roadmap," Pervasive Mob Comput, vol. 23, pp. 1–25, 2015. https://doi.org/10.1016/j.pmcj.2014.12.009.

[106] S. Mishra and S. Jain, "Ontologies as a semantic model in iot," International Journal of Computers and Applications, vol. 42, pp. 233–243, Apr. 2020. https://doi.org/10.1080/1206212X.2018.1504461.

[107] M. F. Gebril, A. M. Maatuk, A. A. Alamrouni, and E. K. Elberkawi, "Transforming relational databases into owl ontology: Methods and perspectives," in Proceeding - 2023 IEEE 3rd International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering, MI-STA 2023, no. May, pp. 452–456, 2023. https://doi.org/10.1109/MI-STA57575.2023.10169181.

[108] B. Xu, L. D. Xu, H. Cai, C. Xie, J. Hu, and F. Bu, "Ubiquitous data accessing method in iot-based information system for emergency medical services," IEEE Trans Industr Inform, vol. 10, no. 2, pp. 1578–1586, 2014. https://doi.org/10.1109/TII.2014.2306382.

[109] A. Kotha, K. Manohar, and V. U, "Iaasi: a device based interoperability as a service for iomt devices," J Ambient Intell Humaniz Comput, vol. 14, no. 10, pp. 14321–14332, 2023. https://doi.org/10.1007/s12652-023-04669-8.

[110] B. J. Hodges, J. T. McDonald, W. B. Glisson, M. Jacobs, M. van Devender, and J. H. Pardue, "Attack modeling and mitigation strategies for risk-based analysis of networked medical devices," in Proceedings of the Annual Hawaii International Conference on System Sciences, vol. 2020-Janua, pp. 6506–6515, 2020. https://doi.org/10.24251/hicss.2020.796.

[111] P. Kumar, G. P. Gupta, and R. Tripathi, "An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for iomt networks," Comput Commun, vol. 166, no. December 2020, pp. 110–124, 2021. https://doi.org/10.1016/j.comcom.2020.12.003.

[112] Y. Otoum, Y. Wan, and A. Nayak, "Federated transfer learning-based ids for the internet of medical things (iomt)," in 2021 IEEE Globecom Workshops, GC Wkshps 2021 - Proceedings, Institute of Electrical and Electronics Engineers Inc., 2021. https://doi.org/10.1109/GCWkshps52748.2021.9682118.

[113] M. Ahmed, S. Byreddy, A. Nutakki, L. F. Sikos, and P. Haskell-Dowland, "Ecu-ioht: A dataset for analyzing cyberattacks in internet of health things," Ad Hoc Networks, vol. 122, no. June, 2021. https://doi.org/10.1016/j.adhoc.2021.102621.

[114] R. Thirumahal, G. S. Sadasivam, and P. Shruti, "Semantic integration of heterogeneous data sources using ontology-based domain knowledge modeling for early detection of covid-19," SN Comput Sci, vol. 3, Nov. 2022. https://doi.org/10.1007/s42979-022-01298-4.

[115] F. W. B. Rivadeneira and O. S. Gómez, "Cybersecurity ontologies: A systematic literature review," Computación e Informática, vol. 9, no. 2, pp. 1–18, 2020. [Online]. Available: https://www.redalyc.org/journal/5122/512267931002/html/.

[116] A. Farquhar, R. Fikes, and J. Rice, "The ontolingua server: a tool for collaborative ontology construction," 1997. [Online]. Available: http://ontolingua.stanford.edu/.

[117] Y. Sure, J. Angele, and S. Staab, "Ontoedit: Multifaceted inferencing for ontology engineering." [Online]. Available: http://www.aifb.uni-karlsruhe.de/WBS/http://www.ontoprise.de/.

[118] "Webode." [Accessed Online: 18 Jan 2024]. Available: https://www.webode.org/.

[119] C. Alrabbaa, F. Baader, S. Borgwardt, R. Dachselt, P. Koopmann, and J. Méndez, "Evonne: Interactive proof visualization for description logics (system description)," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), pp. 271–280, Springer Science and Business Media Deutschland GmbH, 2022. https://doi.org/10.1007/978-3-031-10769-6_16.

[120] N. Noy, S. W. Tu, and M. A. Musen, "Protégé-2000: An open-source ontology-development and knowledge-acquisition environment." [Online]. Available: http://protege.stanford.edu.

[121] A. G. Latha and Y. Srinivas, "Semantic image annotation using ontology and sparql," International Journal of Innovative Technology and Exploring Engineering, vol. 9, no. 3, pp. 3363–3368, 2020. https://doi.org/10.35940/ijitee.h7062.019320.

[122] M. Lissa and V. Bhuvaneswari, Building Knowledge Graph End to End: Data Integration with Semantic Web. Springer Singapore, 2022. https://doi.org/10.1007/978-981-16-4321-7_47.

[123] E. Simperl, R. Krummenacher, and L. Nixon, "A coordination model for triplespace computing," pp. 1–18, 06 2007. https://doi.org/10.1007/978-3-540-72794-1_1.

[124] C. J. Matheus, K. Baclawski, and M. M. Kokar, "Basevisor: A triples-based inference engine outfitted to process ruleml r-entailment rules," 2006.

[125] Netidee, "Combining shacl and ontologies: Shacl and owl," 2023. Accessed: 2024-10-08.

[126] J. Doe and R. Smith, "Shacl4p: Shacl constraints," in Proceedings of the IEEE Conference, IEEE, 2017. Accessed: 2024-10-08.

[127] S. RDF, "Shacl and owl," 2023. Accessed: 2024-10-08.

[128] Ontotext, "What is shacl?," 2023. Accessed: 2024-10-08.

[129] S. Guerfel, N. Ouerhani, and A. Maalel, "Ontology-based representation for emergency management response," in 17th International Conference on INnovations in Intelligent SysTems and Applications, INISTA 2023 - Proceedings, pp. 1–6, 2023. https://doi.org/10.1109/INISTA59065.2023.10310345.

[130] A. Ahmed et al., "Knowledge-based systems survey," International Journal of Academic Engineering Research, vol. 3, no. 7, pp. 1–22, 2019. [Online]. Available: www.ijeais.org/ijaer.

[131] J. B. Ronald and J. L. Hector, Knowledge Representation and Reasoning. Elsevier, 2004.

[132] "Artificial intelligence: A modern approach, 4th us ed.," 2024. [Online]. Available: https://doi.org/10.1109/AIMA.2024.

[133] R. Davis, H. Shrobe, and P. Szolovits, "What is a knowledge representation?," AI Magazine, vol. 14, no. 1, pp. 17–33, 1993. https://ojs.aaai.org/aimagazine/index.php/aimagazine/article/view/1029.

[134] S. Abburu, "A survey on ontology reasoners and comparison," International Journal of Computer Applications, vol. 57, no. 17, 2012.

[135] K. S. Bughio, "Knowledge organization system for partial automation to improve the security posture of iomt networks," Procedia Comput Sci, vol. 225, pp. 3471–3478, 2023. https://doi.org/10.1016/j.procs.2023.10.342.

[136] K. Samuel et al., "Translating owl and semantic web rules into prolog: Moving toward description logic programs," Theory and Practice of Logic Programming, vol. 8, no. 3, pp. 301–322, 2008. https://doi.org/10.1017/S1471068407003249.

[137] R. R. Gorrepati, P. Jonnala, S. R. Guntur, and D. H. Kim, Semantic web of things for healthcare interoperability using IoMT technologies, vol. 1st Editio, pp. 49–82. 2023. https://doi.org/10.1201/9781003441137-3.

[138] F. J. Ruiz-Bertol, D. Rodríguez, and J. Dolado, "Applying rules to an ontology for project management," in Actas de las 16th Jornadas de Ingenieria del Software y Bases de Datos, JISBD 2011, no. January, pp. 257–262, 2011.

[139] T. B. Brown, B. Mann, N. Ryder, M. Subbiah, J. Kaplan, P. Dhariwal, A. Neelakantan, P. Shyam, G. Sastry, A. Askell, S. Agarwal, A. Herbert-Voss, G. Krueger, T. Henighan, R. Child, A. Ramesh, D. M. Ziegler, J. Wu, C. Winter, and D. Amodei, "Language models are few-shot learners," Advances in Neural Information Processing Systems, 2020.

[140] B. Edwards, "Openai's gpt-4 exhibits "human-level performance" on professional benchmarks," Ars Technica, 2023. Archived from the original on March 14, 2023. Retrieved on December 23, 2023.

[141] J. Kim and J. Lee, "How does chatgpt introduce transport problems and solutions in north america?," Transport Findings, 2023. https://doi.org/10.32866/001c.72634.

[142] B. Memarian and T. Doleck, "Chatgpt in education: Methods, potentials, and limitations," Computers in Human Behavior: Artificial Humans, vol. 1, no. 2, 2023. https://doi.org/10.1016/j.chbah.2023.100022.

[143] E. Ferrara, "Genai against humanity: nefarious applications of generative artificial intelligence and large language models," J Comput Soc Sc, 2024. https://doi.org/10.1007/s42001-024-00250-1.

[144] Y. K. Dwivedi et al., "Opinion paper: "so what if chatgpt wrote it?" multidisciplinary perspectives on opportunities, challenges and implications of generative conversational ai for research, practice and policy," International Journal of Information Management, vol. 71, 2023. https://doi.org/10.1016/j.ijinfomgt.2023.102642.

[145] I. Vaccari, V. Orani, A. Paglialonga, E. Cambiaso, and M. Mongelli, "A generative adversarial network (gan) technique for internet of medical things data," Sensors, vol. 21, no. 11, 2021.

[146] G. Lampropoulos, E. Keramopoulos, and K. Diamantaras, "Enhancing the functionality of augmented reality using deep learning, semantic web and knowledge graphs: A review," Visual Informatics, vol. 4, pp. 32–42, Mar. 2020. https://doi.org/10.1016/j.visinf.2020.01.001.

[147] A. Singhal, "Introducing the knowledge graph: things, not strings." https://www.blog.google/products/search/introducing-knowledge-graph-things-not/, 2012. Accessed: Aug. 26, 2023.

[148] L. Wang, C. Sun, C. Zhang, W. Nie, and K. Huang, "Application of knowledge graph in software engineering field: A systematic literature review," Inf Softw Technol, vol. 164, no. September, 2023. https://doi.org/10.1016/j.infsof.2023.107327.

[149] Y. Jia, Y. Qi, H. Shang, R. Jiang, and A. Li, "A practical approach to constructing a knowledge graph for cybersecurity," Engineering, vol. 4, no. 1, pp. 53–60, 2018. https://doi.org/10.1016/j.eng.2018.01.004.

[150] O. Consulting, "An introduction to knowledge representation." Retrieved January 27, 2024.

[151] "Sparql endpoints and how to use them," 2023.

[152] "Semantic university." [Online]. Available: http://dbpedia.org/sparql?

[153] "Sparql 1.1 query language." [Online]. Available: http://www.w3.org/TR/2013/REC-sparql11-query/.

[154] L. Yuan, Y. Bai, Z. Xing, S. Chen, X. Li, and Z. Deng, "Predicting entity relations across different security databases by using graph attention network," in Proceedings - 2021 IEEE 45th Annual Computers, Software, and Applications Conference, COMPSAC 2021, pp. 834–843, 2021. https://doi.org/10.1109/COMPSAC51774.2021.00116.

[155] Z. Liu, X. Q. Di, W. Song, and W. W. Ren, "Vulnerability knowledge extraction method based on joint extraction model," in Proceedings - 2021 9th International Conference on Advanced Cloud and Big Data, CBD 2021, pp. 101–106, 2022. https://doi.org/10.1109/CBD54617.2021.00026.

[156] M. Beyrouti, A. Lounis, B. Lussier, A. Bouadallah, and A. E. Samhat, "Vulnerability and threat assessment framework for internet of things systems," in Proceedings - 2023 6th Conference on Cloud and Internet of Things, CIoT 2023, pp. 62–69, 2023. https://doi.org/10.1109/CIoT57267.2023.10084894.

[157] L. A. B. Sanguino and R. Uetz, "Software vulnerability analysis using cpe and cve," 2017. [Online]. Available:https://doi.org/http://arxiv.org/abs/1705.05347.

[158] K. A. Seale and J. T. McDonald, "Integrating relational data frameworks into risk assessment of networked medical devices," 2017. [Online]. Available: note = https://www.proquest.com/dissertations-theses/integrating-relational-data-frameworks-into-risk/docview/1893567916/se-2?accountid=26642http://link.periodicos.capes.gov.br/sfxlcl41?url_ver=Z39.88-2004&rft_val_fmt=info:ofi/fmt:kev:mtx:dissertation&genre=d.

[159] "Nvd - vulnerability metrics," 2023. [Online]. Available: https://nvd.nist.gov/vuln-metrics.

[160] F. Alsubaei, A. Abuhussein, V. Shandilya, and S. Shiva, "Iomt-saf: Internet of medical things security assessment framework," Internet of Things (Netherlands), vol. 8, Dec. 2019. https://doi.org/10.1016/j.iot.2019.100123.

[161] H. K. M. D. Peters, C. Godfrey, P. McInerney, Z. Munn, and A. C. Tricco, "Chapter 11: Scoping reviews(2020 version). jbi manual for evidence synthesis," tech. rep., 2020. https://doi.org/10.46658/JBIMES-20-12.

[162] F. Khan, M. A. Jan, R. Alturki, M. D. Alshehri, S. T. Shah, and A. U. Rehman, "A secure ensemble learning-based fog-cloud approach for cyberattack detection in iomt," IEEE Trans Industr Inform, vol. 19, no. 10, pp. 10125–10132, 2023. https://doi.org/10.1109/TII.2022.3231424.

[163] P. Radoglou-Grammatikis, P. Sarigiannidis, G. Efstathopoulos, T. Lagkas, G. Fragulis, and A. Sarigiannidis, "A self-learning approach for detecting intrusions in healthcare systems," in IEEE International Conference on Communications, Institute of Electrical and Electronics Engineers Inc., Jun. 2021. https://doi.org/10.1109/ICC42927.2021.9500354.

[164] P. Radoglou-Grammatikis et al., "Modeling, detecting, and mitigating threats against industrial healthcare systems: A combined software defined networking and reinforcement learning approach," IEEE Trans Industr Inform, vol. 18, pp. 2041–2052, Mar. 2022. https://doi.org/10.1109/TII.2021.3093905.

[165] N. I. Haque, M. A. Rahman, and S. I. Ahamed, "Deepcad: A stand-alone deep neural network-based framework for classification and anomaly detection in smart healthcare systems," in Proceedings - 2022 IEEE International Conference on Digital Health, ICDH 2022, no. October 2019, pp. 218–227, 2022. https://doi.org/10.1109/ICDH55609.2022.00042.

[166] V. Ravi, "Deep learning-based network intrusion detection in smart healthcare enterprise systems," Multimed Tools Appl, 2023. https://doi.org/10.1007/s11042-023-17300-x.

[167] A. Rahman et al., "Federated learning-based ai approaches in smart healthcare: concepts, taxonomies, challenges and open issues," Springer US, vol. 26, no. 4, 2023. https://doi.org/10.1007/s10586-022-03658-4.

[168] P. Kulshrestha and T. V. V. Kumar, "Machine learning based intrusion detection system for iomt," International Journal of System Assurance Engineering and Management, no. 0123456789, 2023. https://doi.org/10.1007/s13198-023-02119-4.

[169] A. J. Cartwright, "The elephant in the room: cybersecurity in healthcare," Journal of Clinical Monitoring and Computing, vol. 37, pp. 1123–1132, Oct. 2023. https://doi.org/10.1007/s10877-023-01013-5.

[170] J. Almalki, "State-of-the-art research in blockchain of things for healthcare," Arab J Sci Eng, 2023. https://doi.org/10.1007/s13369-023-07896-5.

[171] J. B. Awotunde, C. Chakraborty, and S. O. Folorunso, A Secured Smart Healthcare Monitoring Systems Using Blockchain Technology, pp. 127–143. 2022. https://doi.org/10.1007/978-3-030-81473-1_6.

[172] H. Szczepaniuk and E. K. Szczepaniuk, "Cryptographic evidence-based cybersecurity for smart healthcare systems," Inf Sci (N Y), vol. 649, no. September, 2023. https://doi.org/10.1016/j.ins.2023.119633.

[173] M. Kumaresan, R. Gopal, M. Mathivanan, and T. Poongodi, Amalgamation of blockchain, IoT, and 5G to improve security and privacy of smart healthcare systems. Elsevier Inc., 2022. https://doi.org/10.1016/B978-0-323-90615-9.00015-3.

[174] M. Mahmood et al., "Improving security architecture of internet of medical things: A systematic literature review," IEEE Access, vol. 11, no. May, pp. 107725–107753, 2023. https://doi.org/10.1109/ACCESS.2023.3281655.

[175] A. Ghourabi, "A security model based on lightgbm and transformer to protect healthcare systems from cyberattacks," IEEE Access, vol. 10, pp. 48890–48903, 2022. https://doi.org/10.1109/ACCESS.2022.3172432.

[176] Y. Otoum, V. Chamola, and A. Nayak, "Federated and transfer learning-empowered intrusion detection for iot applications," IEEE Internet of Things Magazine, vol. 5, no. 3, pp. 50–54, 2022. https://doi.org/10.1109/iotm.001.2200048.

[177] S. Das, T. K. Samal, B. K. Mohanta, and A. Nayak, "Emerging cyber threats in healthcare: A study of attacks in iomt ecosystems," in 2023 7th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), pp. 77–82, IEEE, Oct. 2023. https://doi.org/10.1109/I-SMAC58438.2023.10290147.

[178] A. Aljuhani, A. Alamri, P. Kumar, and A. Jolfaei, "An intelligent and explainable saas-based intrusion detection system for resource-constrained iomt," IEEE Internet Things J, vol. PP, p. 1, 2023.

[179] S. Nandy, M. Adhikari, M. A. Khan, V. G. Menon, and S. Verma, "An intrusion detection mechanism for secured iomt framework based on swarm-neural network," IEEE J Biomed Health Inform, vol. 26, no. 5, pp. 1969–1976, 2022. https://doi.org/10.1109/JBHI.2021.3101686.

[180] J. Nayak, S. K. Meher, A. Souri, B. Naik, and S. Vimal, "Extreme learning machine and bayesian optimization-driven intelligent framework for iomt cyber-attack detection," Journal of Supercomputing, vol. 78, no. 13, pp. 14866–14891, 2022. https://doi.org/10.1007/s11227-022-04453-z.

[181] A. Aljuhani, "Ids-chain: A collaborative intrusion detection framework empowered blockchain for internet of medical things," in Proceedings - 2022 IEEE Cloud Summit, Cloud Summit 2022, pp. 57–62, 2022. https://doi.org/10.1109/CloudSummit54781.2022.00015.

[182] R. M. S. Priya et al., "An effective feature engineering for dnn using hybrid pca-gwo for intrusion detection in iomt architecture," Comput Commun, vol. 160, no. May, pp. 139–149, 2020. https://doi.org/10.1016/j.comcom.2020.05.048.

[183] S. K. Jagatheesaperumal, P. Mishra, N. Moustafa, and R. Chauhan, "A holistic survey on the use of emerging technologies to provision secure healthcare solutions," Computers and Electrical Engineering, vol. 99, no. December 2021, 2022. https://doi.org/10.1016/j.compeleceng.2022.107691.

[184] S. A. Wagan, J. Koo, I. F. Siddiqui, N. M. F. Qureshi, M. Attique, and D. R. Shin, "A fuzzy-based duo-secure multi-modal framework for iomt anomaly detection," Journal of King Saud University - Computer and Information Sciences, vol. 35, no. 1, pp. 131–144, 2023. https://doi.org/10.1016/j.jksuci.2022.11.007.

[185] M. Sills, P. Ranade, and S. Mittal, "Cybersecurity threat intelligence augmentation and embedding improvement - a healthcare usecase," in Proceedings - 2020 IEEE International Conference on Intelligence and Security Informatics, ISI 2020, 2020. https://doi.org/10.1109/ISI49825.2020.9280482.

[186] C. R. Kothari, Research Methodology Methods and Techniques. Jaipur, India, second rev. ed., 1990.

[187] V. R. Basili, "The experimental paradigm in software engineering," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 706 LNCS, pp. 3–12, 1993. https://doi.org/10.1007/3-540-57092-6_91.

[188] A. E. Kelly, R. A. Lesh, and J. Y. Baek, Handbook of Design Research Methods in Education: Innovations in Science, Technology, Engineering, and Mathematics Learning and Teaching (1st ed.). Routledge, 2008. [Online]. Available:https://doi.org/10.4324/9781315759593.

[189] R. D. Galliers, "Research issues in information systems," Journal of Information Technology, vol. 8, pp. 92–98, Jun. 1993. https://doi.org/10.1177/026839629300800204.

[190] J. N. S. Rubí and P. R. de L. Gondim, "Interoperable internet of medical things platform for e-health applications," Int J Distrib Sens Netw, vol. 16, Jan. 2020. https://doi.org/10.1177/1550147719889591.

[191] W. Villegas-Ch, J. García-Ortiz, and I. Urbina-Camacho, "Framework for a secure and sustainable internet of medical things, requirements, design challenges, and future trends," Applied Sciences (Switzerland), vol. 13, no. 11, 2023. https://doi.org/10.3390/app13116634.

[192] Q. Niu, H. Li, Y. Liu, Z. Qin, L. Zhang, and J. Chen, "Toward the internet of medical things: Architecture, trends and challenges," Mathematical Biosciences and Engineering, vol. 21, no. August, pp. 650–678, 2023.

[193] T. Gruber, "Ontology," 1993. [Online]. Available: http://queksiewkhoon.tripod.com/ontology_01.pdf.

[194] J. Barrasa, "Ontologies in neo4j: Semantics and knowledge graphs." Available [Online]: https://neo4j.com/blog/ontologies-in-neo4j-semantics-and-knowledge-graphs/ Accessed on 01-11-2022.

[195] "Snomed ct," 2024. [Online]. Available: https://bioportal.bioontology.org/ontologies/SNOMEDCT. Accessed [ONLINE]: Feb. 12, 2024.

[196] T. M. Corporation, "Structured threat information expression — stixtm," 2013. Available [Online]:https://stix.mitre.org.

[197] D. P. F. Möller, Guide to cybersecurity in digital transformation: Trends, methods, technologies, applications and best practices. Advances in information security, 2023.

[198] "Hitrust," 2024. Available: [Online] https://hitrustalliance.net.

[199] A. Ghubaish, T. Salman, M. Zolanvari, D. Unal, A. Al-Ali, and R. Jain, "Recent advances in the internet-of-medical-things (iomt) systems security," IEEE Internet Things J, vol. 8, pp. 8707–8718, Jun. 2021. https://doi.org/10.1109/JIOT.2020.3045653.

[200] S. El-Sappagh, F. Franda, F. Ali, and K. S. Kwak, "Snomed ct standard ontology based on the ontology for general medical science," BMC Med Inform Decis Mak, vol. 18, Aug. 2018. https://doi.org/10.1186/s12911-018-0651-5.

[201] Kim et al., "Developing a dietary lifestyle ontology to improve the interoperability of dietary data proof-of-concept study," JMIR Form Res, vol. 6, no. 4, 2022.

[202] M. C. Silva, P. Eugénio, D. Faria, and C. Pesquita, "Ontologies and knowledge graphs in oncology research," Cancers, vol. 14, Apr. 2022. https://doi.org/10.3390/cancers14081906.

[203] J. Undercoffer, J. Pinkston, A. Joshi, and T. Finin, "A target-centric ontology for intrusion detection," in The 18th International Joint Conference on Artificial Intelligence in: Workshop on Ontologies in Distributed Systems, pp. 1–8, 2003.

[204] Z. Syed, A. Padia, T. Finin, A. Joshi, and L. Mathews, "Uco: A unified cybersecurity ontology," 2016. Available [ONLINE]: https://www.researchgate.net/publication/287195565.

[205] B. A. Mozzaquatro, C. Agostinho, D. Goncalves, J. Martins, and R. Jardim-Goncalves, "An ontology-based cybersecurity framework for the internet of things," Sensors (Switzerland), vol. 18, Sep. 2018. https://doi.org/10.3390/s18093053.

[206] R. Neches et al., "Enabling technology for knowledge sharing ai magazine volume 12 number 3 (1991) (© aaai)," AI Magazine, vol. 12, no. 3, 1991.

[207] H. S. Pinto and J. P. Martins, "Ontologies: How can they be built?," Knowl Inf Syst, vol. 6, pp. 441–464, Jul. 2004. https://doi.org/10.1007/s10115-003-0138-1.

[208] E. Adel, S. El-Sappagh, S. Barakat, and M. Elmogy, Ontology-based electronic health record semantic interoperability: A survey. Elsevier Inc., 2019. https://doi.org/10.1016/b978-0-12-815370-3.00013-x.

[209] P. Szeredi, G. Lukácsy, and T. Benkő, "Description logic," in The Semantic Web Explained: The Technology and Mathematics behind Web 3.0, pp. 175–245, Cambridge University Press, 2014. https://doi.org/10.1017/cbo9781139194129.005.

[210] X. Zhu, B. Liu, C. Zhu, Z. Ding, and L. Yao, "Approximate reasoning for large-scale abox in owl dl based on neural-symbolic learning," Mathematics, vol. 11, Feb 2023. https://doi.org/10.3390/math11030495.

[211] Z. Tang, S. Pei, X. Peng, F. Zhuang, X. Zhang, and R. Hoehndorf, "Tar: Neural logical reasoning across tbox and abox," 2022. [Online]. Available: http://arxiv.org/abs/2205.14591.

[212] N. F. Noy and D. L. McGuinness, Ontology Development 101: A Guide to Creating Your First Ontology. 2001.

[213] S. Rudolph, "Foundations of description logics," Lecture Notes in Computer Science, vol. 6848, pp. 76–136, 2011.

[214] A. Kumar and G. Deepak, "Hetonto: A novel approach for conceptualization, modeling, visualization, and formalization of domain centric ontologies for heat transfer," in Proceedings of CONECCT 2020 - 6th IEEE International Conference on Electronics, Computing and Communication Technologies, 2020. https://doi.org/10.1109/CONECCT50063.2020.9198413.

[215] A. E. Schütz, T. Fertig, and K. Weber, "Defining a core ontology for medical devices in germany to ensure semantic interoperability," in Communications in Computer and Information Science, vol. 1341, pp. 394–410, 2021. https://doi.org/10.1007/978-3-030-68527-0_25.

[216] Z. Faycal and T. Abdelkamel, "Building a semantic web services ontology in the pharmaceutical field using the owl-s language," pp. 8–15, 2021. https://doi.org/10.1109/ICISAT54145.2021.9678408.

[217] A. Gómez-Pérez, M. Fernández, and A. de Vicente, "Towards a method to conceptualize domain ontologies," in Ontological Engineering 12th European Conference on Artificial Intelligence (ECAI'96), no. April 2000, pp. 41–51, 1996.

[218] C. M. Keet, Open World Assumption. 2013. https://doi.org/10.1007/978-1-4419-9863-7_734#citeas.

[219] E. Sirin, B. Parsia, B. C. Grau, A. Kalyanpur, and Y. Katz, "Pellet: A practical owl-dl reasoner," Journal of Web Semantics, vol. 5, pp. 51–53, Jun. 2007. https://doi.org/10.1016/J.WEBSEM.2007.03.004.

[220] Z. Li, M. C. Yang, and K. Ramani, "A methodology for engineering ontology acquisition and validation," Research in Engineering Design, vol. 23, no. 1, 2009. https://doi.org/10.1017/S0890060409000092.

[221] D. Spoladore and E. Pessot, "Collaborative ontology engineering methodologies for the development of decision support systems: Case studies in the healthcare domain," Electronics (Switzerland), vol. 10, no. 9, 2021. https://doi.org/10.3390/electronics10091060.

[222] F. Z. Hannou, F. Atigui, N. Lammari, and S. S. said Cherfi, "Safecareonto: A cyber-physical security ontology for healthcare systems," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), pp. 22–34, Springer Science and Business Media Deutschland GmbH, 2021. https://doi.org/10.1007/978-3-030-86475-0_3.

[223] C. Roussey, F. Pinet, M. A. Kang, and O. Corcho, An introduction to ontologies and ontology engineering, vol. 1, pp. 9–38. Springer London, 2011. https://doi.org/10.1007/978-0-85729-724-2_2.

[224] E. F. Kendall and D. L. McGuinness, Ontology Engineering. Springer, 2022.

[225] L. P. Santamaría, D. F. Lobón, A. J. Díaz-Honrubia, E. M. Ruiz, S. Nifakos, and A. Rodríguez-González, "Towards the representation of network assets in health care environments using ontologies," Methods Inf Med, 2021. https://doi.org/10.1055/s-0041-1735621.

[226] S. M. Rashid et al., "The semantic data dictionary – an approach for describing and annotating data," Data Intell, vol. 2, pp. 443–486, Oct. 2020. https://doi.org/10.1162/dint_a_00058.

[227] L. H. Karlsen, "Description logic 1: Syntax and semantics." [Online]. Available: note = http://www.uio.no/studier/emner/matnat/ifi/INF3170/h15/undervisningsmateriale/dl1.pdf.

[228] F. Baader and W. Nutt, "Basic description logics," in The Description Logic Handbook: Theory, Implementation and Applications (F. Baader, D. Calvanese, D. L. McGuinness, D. Nardi, and P. F. Patel-Schneider, eds.), pp. 47–100, Cambridge, UK: Cambridge University Press, 2010. [Online]. Available: note = https://doi.org/10.1017/cbo9780511711787.004.

[229] T. Fotis, K. Kioskli, A. Sundaralingam, A. Fasihi, and H. Mouratidis, "Co-creation in a digital health living lab: A case study," Front Public Health, vol. 10, no. 9, 2023. [Online]. Available: note = https://doi.org/10.3389/fpubh.2022.892930.

[230] K. Hofer-Schmitz and B. Stojanović, "Towards formal verification of iot protocols: A review," Computer Networks, vol. 174, p. 107233, 2020. https://doi.org/10.1016/j.comnet.2020.107233.

[231] K. Keerthi, I. Roy, A. Hazra, and C. Rebeiro, Formal verification for security in IoT devices, pp. 179–200. Springer International Publishing, 2019. https://doi.org/10.1007/978-3-030-02807-7_9.

[232] M. Krichen, "A survey on formal verification and validation techniques for internet of things," Applied Sciences (Switzerland), vol. 13, Jul. 2023. https://doi.org/10.3390/app13148122.

[233] A. Souri and M. Norouzi, "A state-of-the-art survey on formal verification of the internet of things applications," Journal of Service Science Research, vol. 11, pp. 47–67, Jun. 2019. https://doi.org/10.1007/s12927-019-0003-8.

[234] R. Dwivedi, D. Mehrotra, and S. Chandra, "Potential of internet of medical things (iomt) applications in building a smart healthcare system: A systematic review," J Oral Biol Craniofac Res, vol. 12, pp. 302–318, Mar. 2022. https://doi.org/10.1016/j.jobcr.2021.11.010.

[235] I. Jayatilleka and M. N. Halgamuge, Internet of Things in healthcare: Smart devices, sensors, and systems related to diseases and health conditions. Elsevier Inc., 2019. https://doi.org/10.1016/B978-0-12-818014-3.00001-2.

[236] S. Zakerabasali and S. M. Ayyoubzadeh, "Internet of things and healthcare system: A systematic review of ethical issues," Health Sci Rep, vol. 5, no. 6, 2022. https://doi.org/10.1002/hsr2.863.

[237] S. B. Far and A. I. Rad, "Internet of artificial intelligence (ioai): the emergence of an autonomous, generative, and fully human-disconnected community," Discover Applied Sciences, vol. 6, Feb. 2024. https://doi.org/10.1007/s42452-024-05726-3.

[238] F. Alsubaei, A. Abuhussein, and S. Shiva, "Ontology-based security recommendation for the internet of medical things," IEEE Access, vol. 7, pp. 48948–48960, 2019. https://doi.org/10.1109/ACCESS.2019.2910087.

[239] S. Qin and K. P. Chow, Automatic Analysis and Reasoning Based on Vulnerability Knowledge Graph. Springer Singapore, 2019. https://doi.org/10.1007/978-981-15-1922-2.

[240] R. Christian, S. Dutta, Y. Park, and N. Rastogi, "An ontology-driven knowledge graph for android malware," in Proceedings of the ACM Conference on Computer and Communications Security, pp. 2435–2437, 2021. https://doi.org/10.1145/3460120.3485353.

[241] K. S. Bughio, D. M. Cook, and S. A. A. Shah, "Generative ai models in rule-based systems: Testing and evaluation," in Proceedings of the 28th Annual KES Conference, (Seville, Spain), September 11-13 2024. Accepted in https://kes2024.kesinternational.org/.

[242] B. Robert and E. B. Brown, Ontologies for Agents: Theory and Experiences, vol. 1. 2004.

[243] "Loading and saving rdf reading rdf files." [Online]. Available: https://rdflib.readthedocs.io/en/stable/intro_to_parsing.html.

[244] L. Bracciale, P. Loreti, and G. Bianchi, "Cybersecurity vulnerability analysis of medical devices purchased by national health services," Sci Rep, vol. 13, no. 1, pp. 1–12, 2023. https://doi.org/10.1038/s41598-023-45927-1.

[245] "If…then… and it is not the case that… – a concise introduction to logic," 2024. [Online]. Available: note = https://milnepublishing.geneseo.edu/concise-introduction-to-logic/chapter/2-ifthen-and-it-is-not-the-case-that/.

[246] "protégé," 2023. [Online]. Available: note = https://protege.stanford.edu/software.php#desktop-protege.

[247] F. Ali et al., "Type-2 fuzzy ontology–aided recommendation systems for iot–based healthcare," Comput Commun, vol. 119, no. August 2017, pp. 138–155, 2018. https://doi.org/10.1016/j.comcom.2017.10.005.

[248] "Rdf - semantic web standards," 2023. [Online]. Available:https://www.w3.org/RDF/.

[249] J. Yu, J. A. Thom, and A. Tam, "Lncs 3761 - evaluating ontology criteria for requirements in a geographic travel domain," pp. 41–52, 2005. [Online]. Available: note = http://www.lonelyplanet.com.

[250] M. Amith, Z. He, J. Bian, J. A. Lossio-Ventura, and C. Tao, "Assessing the practice of biomedical ontology evaluation: Gaps and opportunities," Journal of Biomedical Informatics, vol. 80, pp. 1–13, Apr. 2018. https://doi.org/10.1016/j.jbi.2018.02.010.

[251] A. Johnson, T. Pollard, and R. Mark, "Mimic-iii clinical database." https://doi.org/10.13026/C2XW26.

[252] B. Aldughayfiq, F. Ashfaq, N. Z. Jhanjhi, and M. Humayun, "Capturing semantic relationships in electronic health records using knowledge graphs: An implementation using mimic iii dataset and graphdb," Healthcare (Switzerland), vol. 11, Jun 2023. https://doi.org/10.3390/healthcare11121762.

Appendix A

List of Vendors, Products, Medical devices and Tecnology

Table A.1: List of Vendors Providing Medical Devices in Healthcare with Technology

Vendors, Products, Medical Device			
Vendors	**Products**	**Medical Device**	**Technology**
Abbott[1]	Cardiac Rhythm Management	MRI compatible pacemakers, Implantable cardiac monitors, Remote monitoring systems	Bluetooth
	Glucose monitoring system	FreeStyle Libre Sensor[2] (Sensor glucose monitoring)	
Vitalconnect	VitalPatch[3]	Wearable, 11 measurements: Temperature, ECG, Heart rate, Posture, HR variability, Fall detection, Respiratory rate, Activity, Blood pressure, Oxygen saturation, Weight	Cloud-based analysis
Foracare [4] [5]	D40g, GTel, Premium V10 BLE, P20B and others	2-in-1 Blood Pressure, Blood Glucose Monitoring System, FORA TeleHealth Software	Cellular or Bluetooth, Cloud

Continued on next page

[1]https://www.aus.abbott/
[2]https://www.freestylelibre.com.au/
[3]https://vitalconnect.com/remote-patient-monitoring/
[4]https://foracare.com/remote-patient-monitoring/
[5]https://foracare.com/telehealth-devices/

Table A.1 – continued from previous page

Vendors	Products	Medical Device	Technology
Philips	HealthSuit[6] Digital Platform (HSDP) solution, ETrac[7], eCac[8]	Not available	Cloud-based connectivity
Alivetech	AlivecorKardiaMobile 6L ECG	Wearable 6 Lead EKG (electrocardiogram) connected with Android and iOS	Bluetooth
Neurotech	Mente	Wearable therapeutic tool for autism	Connected with Android and iOS, Bluetooth
Apple	Smartwatch 5 and 7 series	Heart rate monitor, Blood oxygen app, ECG app, International Emergency calling, Fall detection	Bluetooth, WiFi, Cellular
Omron	Not available	Environmental sensor, Temperature, Humidity, Light, UVI, Pressure, Noise, Acceleration	Bluetooth
Mysignals[9]	Libelium	17 sensors including glucometer, body position, blood pressure	Bluetooth, Wi-Fi, Cloud-based
Comarch	Comarch HomeHealth[10]	ECG, Blood Pressure, Thermometer, Glucometer	Not available
Validic	Validic Impact[11]	Not available	Bluetooth, Apple Health, Google Fit services
	VitalSnap[12] Captures photos, digitizes and uploads on Validic API	Not available	Optical Character Recognition (OCR) using mobile phone camera

Continued on next page

[6]https://aws.amazon.com/solutions/case-studies/philips-healthsuite-digital-platform-case-study/
[7]https://www.philips.com.au/healthcare/e/enterprise-telehealth/etrac
[8]https://www.philips.com.au/healthcare/e/enterprise-telehealth/ecac
[9]http://www.my-signals.com/
[10]https://www.comarch.com/healthcare/products/comarch-homehealth/
[11]https://validic.com/solutions/impact/
[12]https://validic.com/solutions/mobile-solutions/

Table A.1 – continued from previous page			
Vendors	**Products**	**Medical Device**	**Technology**
Tele2iot	Cuviva tools/solution[13]	Weight, Blood pressure, Saturation, Pulse, Fever thermometer, Blood sugar level sensors	2CONTROL (Cisco IoT Control Center) to manage SIMs and connectivity, secure data transfer via private VPN
Vitls	Vitls[14]	Patient vitals including Pulse, SPO2, Respiration, Temperature	HIPAA-compliant cloud database, Compatible with iOS, Android, Web browsers, EHRs (Electronic Health Records)
iHealth	iHealth Nexus[15], iHealth Lancets	Blood pressure, Diabetes	Bluetooth connection with smartphone via app

[13]https://tele2iot.com/case/tele2-iot-cuviva-connected-healthcare/
[14]https://www.vitlsinc.com/
[15]https://www.ihealthlabs.com.au/shop/category/all-products/6024

Appendix B

Selected Studies for Scoping Review

Table B.1: Comparison of studies based on proposed criteria related to Technologies, Area of Research (AoR), Knowledge Organization Systems (KOS), Automated Reasoning (AR), Cyberattacks/Vulnerability Detection (C/VD), and Knowledge Graph Representation (KGR).

Comparison of Studies									
No	**Author**	**Database**	**Technologies**	**Motive**	**AoR**	**KOS**	**AR**	**C/VD**	**KGR**
1	Khan et al. 2023	IEEE Xplore Digital Library	Ensemble learning and fog computing	It highlights the increasing risk of cyber-attacks and the constraints of traditional, independent cloud-based security in the context of the Internet of Medical Things (IoMT). The suggestion is to implement an intrusion detection system based on ensemble learning, utilizing a fog-cloud architecture to identify harmful activities within IoMT environments.	IoMT	No	No	Yes (IDS)	No

Continued on next page

Table B.1 – continued from previous page									
No	**Author**	**Database**	**Technologies**	**Motive**	**AoR**	**KOS**	**AR**	**C/VD**	**KGR**
2	Mahmood et al. 2023	IEEE Xplore Digital Library	SLR (System Literature Review), Python interface Model	To address the security challenges in IoMT	IoMT	No	No	Yes-Python Interface	No
3	Weber et al. 2023	IEEE Xplore Digital Library	Kitchenham et al. for SLRs in software engineering	To address the growing threat of cyber-attacks in hospitals, focusing on medical cyber-physical systems (MCPS).	Medical cyber-physical systems (MCPS)	No	No	Yes (IDS)	No
4	Radoglou-Grammatikis et al. 2021	IEEE Xplore Digital Library	ML/DL specifically Active Learning	An intrusion detection and prevention system (IDPS) framework designed for medical service scenarios employing HTTP and Modbus/TCP protocols.	IoMT/ Medical services	No	No	Yes (IDS) HTTP/TCP cyberattacks	No
5	Haque, Rahman, and Ahamed 2022	IEEE Xplore Digital Library	Deep Neural Network (DNN)	To enhance the security of Smart healthcare systems (SHSs) by integrating anomaly detection directly into the DNN model used for patient status classification	IoMT	No	No	Anomaly Detection (ML-DNN)	No
6	Ghourabi 2022	IEEE Xplore Digital Library	LightGBM model and a Tranformer-based model	To ensure the security of the entire network regardless of the devices and computers installed.	Healthcare	No	No	Yes (IDS, Malware detection)	No

Continued on next page

Table B.1 – continued from previous page

No	Author	Database	Technologies	Motive	AoR	KOS	AR	C/VD	KGR
7	Otoum, Wan, and Nayak 2021	IEEE Xplore Digital Library	Federated Transfer Learning-based (FTL-based), DNN (Deep Neural Network)	To secure the patient's healthcare-connected devices.	IoMT	No	No	Yes (FTL-IDS)	No
8	Otoum, Chamola, and Nayak 2022	IEEE Xplore Digital Library	Fault-Tolerant Learning (FTL)-based, CNN, DNN	To enhance the security of healthcare-connected devices	IoMT	No	No	Yes (Fault-Tolerant Learning (FTL)-based Intrusion Detection System (IDS))	No
9	Das et al. 2023	IEEE Xplore Digital Library (REVIEW)	ML-Based (i.e., IDS), Blockchain	To address the diverse challenges presented by cyberattacks on the Internet of Medical Things (IoMT).	IoMT Ecosystem	No	No	Yes (IDS-Blockchain)	No
10	Aljuhani 2022	IEEE Xplore Digital Library	Blockchain, Fog Computing	To propose IDS-Chain, collaborative intrusion detection framework empowered blockchain technology for protecting IoMT networks.	IoMT	No	No	Yes (IDS-Fog Computing)	No

Continued on next page

Table B.1 – continued from previous page									
No	**Author**	**Database**	**Technologies**	**Motive**	**AoR**	**KOS**	**AR**	**C/VD**	**KGR**
11	Radoglou-Grammatikis 2022	IEEE Xplore Digital Library	Machine learning (ML) and software defined networking (SDN)	To address cybersecurity concerns associated with the IEC 60 870-5-104 protocol in industrial healthcare systems.	IoMT	No	No	Yes (ML techniques)	No
12	Aljuhani et al. 2023	IEEE Xplore Digital Library	Particle Swarm Optimization (PSO), Software as a Service (SaaS), Ensemble ML and DL, SHapley Additive exPlanations (SHAP)	To secure the patients data and device integrity and enhance the trust in healthcare system.	IoMT	No	No	Yes (Ensemble ML and DL)	No
13	Nandy et al. 2022	IEEE Xplore Digital Library	Swarm-Neural Network (Swarm-NN)	To identify the attacks during data transmission through a network and analyze the health data efficiently at the edge of the network with higher accuracy.	IoMT	No	No	Yes (IDS-Swarm-Neural Network (Swarm-NN))	No
14	Nguyen et al. 2021	IEEE Xplore Digital Library	Mobile Edge Computing (MEC), Blockchain	To enhance efficiency and security of IoMT	IoMT	No	No	Yes (MEC and Blockchain)	No
Continued on next page									

Table B.1 – continued from previous page

No	Author	Database	Technologies	Motive	AoR	KOS	AR	C/VD	KGR
15	Almalki 2023	Springer Link	Blockchain	A survey paper to analyze current state-of-the-art blockchain work in several IoT disciplines, with a focus on the health sector.	e-Health	No	No	YES (Blockchain)	No
16	Nayak et al. 2022	Springer Link	Bayesian optimization and extreme learning machine (ELM)	To propose an IoMT framework with the hybridization of Bayesian optimization and extreme learning machine (ELM) to encourage the performance with enhanced accuracy in decision-making process compared to similar state-of-the-art methods.	IoMT	No	No	Yes (Bayesian optimization and extreme learning machine (ELM))	No
17	Rahman et al. 2023	Springer Link	Federated Learning (FL), Artificial Intelligence (AI), and Explainable Artificial Intelligence (XAI).	This survey thoroughly examines the latest developments in FL, AI, XAI, and e-Healthcare, focusing on key issues like security, privacy, reliability, scalability, and confidentiality and outlining potential research areas and future directions for FL-based AI in healthcare management.	e-Health	No	No	Yes (Federated Learning (FL, Blockchain)	No

Continued on next page

Table B.1 – continued from previous page									
No	**Author**	**Database**	**Technologies**	**Motive**	**AoR**	**KOS**	**AR**	**C/VD**	**KGR**
18	Ravi 2023	Springer Link	Network-based Intrusion Detection Systems (N-IDS), convolutional neural network (CNN) and long short-term memory (LSTM)	To propose a multidimensional attention-based deep learning approach for Network-based Intrusion Detection Systems (N-IDS), achieving high accuracy in detecting attacks across diverse network environments.	Smart Healthcare enterprise system	No	No	Yes (Network-based Intrusion Detection Systems (N-IDS))	No
19	Kulshrestha and Vijay Kumar 2023	Springer Link	ML-Based Intrusion detection System (IDS), Adaptive boosting based IDS	Machine Learning (ML) oriented Intrusion Detection System (IDS) constructed to identify cyber-attacks in IoMT systems.	IoMT	No	No	Yes- Machine Learning (IDS)	No
20	Awotunde, Chakraborty, and Folorunso 2022	Springer Link	Blockchain	A smart healthcare monitoring system proposed with intelligence and security features. It utilizes blockchain technology to safeguard the IoT-based system operating on the cloud.	Smart Healthcare monitoring	No	No	Yes- Blockchain	No
Continued on next page									

Table B.1 – continued from previous page

No	Author	Database	Technologies	Motive	AoR	KOS	AR	C/VD	KGR
21	Cartwright 2023	Springer Link	Awareness about cyber-attacks and vulnerabilities	The paper discusses the general landscape of cybersecurity in healthcare, including the risks posed by AI and the challenges brought by the COVID-19 pandemic.	Protected Health Information (PHI)	No	No	No	No
22	Wazid and Gope 2023	ACM Digital Library	Access control, key management, blockchain	An IoMT-based e-healthcare system BACKM-EHA proposed, and security analysis proved its resilience against the various types of possible attacks through the standard, i.e., "Real-Or-Random model".	E-Healthcare	No	No	Yes Blockchain	No
23	Swarna Priya et al. 2020	Science Direct	Deep Neural Network (DNN), Grey-Wolf Optimization algorithm	To develop a robust Intrusion Detection System (IDS) within IoMT context for the identification and prediction of unforeseen cyberattacks.	IoMT	No	No	Yes (IDS-DNN)	No
24	Szczepaniuk 2023	Science Direct	Blockchain	Introduces algorithms designed to generate, execute, and validate smart contracts tailored for the processing of medical data within Electronic Health Records (EHRs).	smart healthcare systems (SHSs)	No	No	Risk Analysis method-Blockchain	No

Continued on next page

Table B.1 – continued from previous page									
No	**Author**	**Database**	**Technologies**	**Motive**	**AoR**	**KOS**	**AR**	**C/VD**	**KGR**
25	Kumar, Gupta, and Tripathi 2021	Science Direct	Ensemble learning approach, Fog Cloud architecture	The proposed system used to enhance the security of IoMT networks, ensuring the reliability and safety of critical healthcare systems and patient data.	IoMT	No	No	Yes- ensemble learning approach	No
26	Jagath et al. 2022	Science Direct	Internet of Things (IoT), 5G networks, artificial intelligence (AI), and big data analytics	To provide a comprehensive survey on the use of modern enabling technologies, such as the Internet of Things (IoT), 5G networks, artificial intelligence (AI), and big data analytics, for providing secure and resilient healthcare solutions.	Healthcare	No	No	No	No
27	Wagan et al. 2023	Science Direct	Fuzzy C-Means clustering, Bi-LSTM technique	The Duo-Secure IoMT framework employs data from multi-modal sensory signals to distinguish between attack patterns and regular data from IoMT devices.	IoMT	No	No	Anomaly detection (Fuzzy C-Means clustering, Bi-LSTM technique)	No
Continued on next page									

Table B.1 – continued from previous page

No	Author	Database	Technologies	Motive	AoR	KOS	AR	C/VD	KGR
28	Gaba et al. 2022	Science Direct	Zero-Knowledge Proofs	An innovative mutual authentication and key agreement protocol proposed for securing critical healthcare applications on the Internet of Things (IoT), utilizing Zero-Knowledge Proofs.	Internet of Healthcare applications (IoHA)	No	No	Yes (penetration testing)	No
29	Kumaresan et al. 2022	Science Direct	Blockchain, 5G	To focus on utilizing 5G technology for the monitoring and care of patients affected by a spectrum of diseases ranging from common to severe.	Healthcare	No	No	Yes Blockchain	No
30	Sills, Ranade, and Mittal 2020	Scopus	Augmentation and embedding	This system compiles Cyber Threat Intelligence on medical devices and their vulnerabilities from sources like manufacturers and ICS-CERT, enhancing the intelligence repository.	Healthcare	Yes	No	Yes (Augmentation)	Yes

Continued on next page

Table B.1 – continued from previous page									
No	**Author**	**Database**	**Technologies**	**Motive**	**AoR**	**KOS**	**AR**	**C/VD**	**KGR**
31	Banyal et al. 2022	Scopus	Computational Intelligence	This research gives an overview of Computational Intelligence applications in biomedicine while addressing challenges associated with their integration into medical applications.	IoMT	No	No	Yes (Computational Intelligence)	No

Appendix C

Python Script for Integrating CVE Data into MIoT Ontology

```
import json
from owlready2 import *

# Load your ontology
onto_path.append(r"D:\NEW")
onto_file_path = r"abc.owl"
onto = get_ontology(onto_file_path)

# Check if ontology loading was successful
if onto is None:
   print("Failed to load the ontology! Please check the file path and format.")
   exit()

try:
   # Load the ontology
   onto.load()

   # Load NVD CVE data from JSON file
   with open(r'abc\NVD Scripts\nvdcve-1.1-modified.json', encoding='utf-8') as f:

      data = json.load(f)

   # Iterate through CVE entries and create instances
   for entry in data['CVE_Items']:
      cve_id = entry['cve']['CVE_data_meta']['ID']
      description = entry['cve']['description']['description_data'][0]['value']
      # Extract other relevant information as needed

      # Create instance of CVE class
      cve_instance = onto.CVE(cve_id)
      cve_instance.description = description
      # Set other properties accordingly
```

```
    # Save the ontology
    onto.save(file=onto_file_path, format="rdfxml") # Adjust format as needed
    print("Ontology updated successfully.")
except Exception as e:
    print("An error occurred:", e)
```

Listing C.1: Python Script for Integrating CVE Data into MIoT Ontology